

ЗАКОН ЗА КЛАСИФИЦИРАНИ ИНФОРМАЦИИ

ГЛАВА ПРВА ОПШТИ ОДРЕДБИ

Член 1

Со овој закон се поставуваат основните принципи врз кои се заснова системот за безбедност на класифицирани информации кој е дел од надлежностите на органите на државната управа на Република Македонија поврзани со јавната безбедност, одбраната, надворешните работи или разузнавачките и безбедносните активности на земјата.

Со овој закон се уредуваат: класификацијата на информациите, условите, критериумите, мерките и активностите што се преземаат за нивна заштита и безбедност, правата, обврските и одговорноста на создавачите и корисниците на класифицирани информации, меѓународната размена, инспекцискиот надзор над спроведувањето на овој закон, како и други прашања во врска со пристапот и ракувањето со класифицирани информации.

Овој закон е обврзувачки за органите на државната управа, органите на локалната самоуправа, јавните претпријатија и други органи и институции, како и за физичките и правните лица и комуникациските оператори, заради законски обврски и/или реализација на класифицирани договори со органите на државната управа и институциите.

Член 2

Обврска за заштита на класифицираните информации имаат сите што имале пристап и/или биле запознаени со нивната содржина.

Член 3

Целта на овој закон е обезбедување на законито користење на класифицирани информации и оневозможување на секаков вид незаконит или неовластен пристап и злоупотреба на информациите.

Член 4

Одредбите од овој закон ќе се применуваат како во поглед на националните класифицирани информации, така и во поглед на класифицираните информации примени од странски држави и меѓународни организации или создадени во меѓусебна соработка, доколку со ратификуваните меѓународни договори или со меѓународните договори на кои им пристапила Република Македонија, поинаку не е уредено.

Член 5

За спроведување на целите на овој Закон, за заштита на класифицираните информации и меѓународните стандарди, за реализирање на размената на класифицирани информации согласно со меѓународните договори, за вршење инспекциски надзор над спроведувањето на одредбите на овој закон и другите прописи од областа на класифицираните информации, како и за вршење на други работи утврдени со овој закон, е надлежна Дирекцијата за безбедност на класифицирани информации (во натамошниот текст: Дирекција).

Значење на изразите употребени во овој закон

Член 6

Одделни изрази употребени во овој закон го имаат следново значење:

1. „Информација“ е сознание кое може да биде пренесено во било која форма.
2. „Информација од интерес за Република Македонија“ е секоја информација изготвена од орган на државната управа, орган на единица на локалната самоуправа, институција, јавно претпријатие, јавна установа и служба, физичко или правно лице, како и од странски државен орган, односно странско физичко или правно лице, која се однесува на безбедноста и одбраната на државата, нејзиниот територијален интегритет и суверенитет, уставниот поредок, јавниот интерес, и слободите и правата на човекот и граѓанинот.
3. „Класифицирана информација“ е информација или средство од делокругот на работа на орган на државната управа, институции или други правни лица која што се однесува на јавната безбедност, одбраната, надворешните работи или безбедносни или разузнавачки активности на државата која согласно со закон мора да се заштити од неовластен пристап и е обележана со соодветен степен на класификација во согласност со овој закон. Класифицирани информации може да претставуваат документи, технички средства, машини, опрема, односно одвоени компоненти или оружје или алати што се произведени или се во процес на производство.
4. „Документ“ е секој пишан текст, нацрт или скица, репродукција, копија, фотографија, аудио, видео, магнетски, електронски, оптички или друг вид на запис.
5. „Штета“ е повреда на интересите на државата како последица од загрозување на безбедноста на класифицираните информации од интерес за Република Македонија или информациите кои Република Македонија е обврзана да ги заштитува согласно со меѓународни договори.
6. „Безбедносен ризик“ е можност за нарушување на безбедноста на класифицираната информација.
7. „Безбедност на класифицирана информација“ е збир на активности и мерки со кои се обезбедува заштитата на класифицираните информации од неовластен пристап и неовластено ракување.
8. „Безбедносен сертификат за физичко лице“ е документ со кој се потврдува дека за физичкото лице не постои безбедносен ризик за пристап и ракување со класифицирани информации.
9. „Безбедносен сертификат за правно лице“ е документ со кој се потврдува дека за правното лице не постои безбедносен ризик и дека поседува физички или

организациски капацитети за ракување со класифицирани информации и/или за чување на класифицирани информации, согласно со закон.

10. „Дозвола за пристап до класифицирани информации“ е документ со кој се потврдува дека странското физичко или правно лице има безбедносен сертификат издаден во матичната држава и има право на пристап и користење на класифицирани информации во Република Македонија.

11. „Потребно е да знае“ е принцип според кој се утврдува корисникот кој има потреба за пристап до класифицирани информации заради извршување на функцијата или на службената должност и службените овластувања, на дејноста или за спроведување на класифицирани договори.

12. „Создавач на класифицирана информација“ е овластен изработувач на класифицирана информација. Создавачи на класифицирани информации се органите на државната управа, органите на единиците на локалната самоуправа, институции и други физички или правни лица, што создаваат информации од значење за јавната безбедност, одбраната, надворешните работи и безбедносните и разузнавачките активности на органите на државната управа на Република Македонија.

13. „Дисеминација на класифицирани информации“ претставува распоредување на класифицирани информации согласно принципот "потребно е да знае" до лица кои поседуваат соодветен безбедносен сертификат.

14. „Корисник на класифицирана информација“ е физичко или правно лице кое има потреба за пристап до класифицирани информации заради извршување на функцијата, службената должност и службените овластувања или за спроведување на класифицирани договори и кое има безбедносен сертификат.

16. „Ракување со класифицирани информации“ е процес кој го опфаќа секое постапување со класифицираните информации во времетраење на нивното постоење. Тоа подразбира нивно создавање, евиденција, пренос, користење, рекласификација, декласификација, архивирање и уништување.

17. „Безбедносен појас“ е простор околу објектот којшто претставува минимална оддалеченост од објектот од која можат да бидат загрозени објектот и класифицираните информации во него.

18. „Безбедносна зона“ е простор или просторија во објектот во кој се ракува и во кој се чуваат класифицирани информации до степенот "државна тајна" и има потреба од соодветна физичка заштита.

19. „Административна зона“ е јасно определен заштитен простор што се воспоставува околу или пред безбедносните зони во коишто постојат можности за контрола на лица и возила.

20. „Класифициран договор“ е секој облик на договор или договор кој произлегува од него, вклучувајќи ги и преговорите за склучување на истиот, којшто содржи или овозможува пристап до класифицирани информации.

21. „Офицер за безбедност на класифицирани информации“ е лице овластено од носителот на јавна функција или од одговорното лице во институцијата или во правното лице кое има должност да се грижи за ефикасно и координирано извршување на правата и обврските кои произлегуваат од овој закон.

22. „Криптографска безбедност“ е компонента на безбедноста на комуникациско - информациските системи која ја опфаќа криптографската заштита, управувањето со криптографските материјали и развојот на методи на криптографска заштита.
23. „Криптографска заштита“ е систем на криптографски материјали и производи кои се користат за заштита на класифицирани информации од неовластен пристап при ракување и чување на класифицираните информации.
24. „Криптографски производ“ е софтвер или уред со кој се врши криптографска заштита.
25. „Криптографски материјали (крипто материјали)“ се криптографски алгоритми, криптографски хардверски и софтверски модули, крипто клучеви, насоките за нивна имплементација и придружната документација.
27. „Безбедносна акредитација на комуникациско-информациски системи“ е процес на формално одобрување на комуникациско-информациски системи за работа до одредениот степен на класификација, во посебни безбедносни услови во неговото оперативно опкружување и на прифатливо ниво на ризик.
28. „Процес на управување со ризик“ е процес на идентификација, контролирање и минимизирање на настани што можат да влијаат врз безбедноста на една организација или на системот што таа го користи. Процесот ги вклучува сите активности што се поврзани со ризици, вклучувајќи проценка, третирање, прифаќање и комуникација.
29. „Комуникациско-информациски систем (КИС)“ е секој систем што овозможува создавање, чување, обработка или пренос на информациите во електронска форма. КИС ги вклучува сите средства потребни за негово функционирање, како инфраструктурата, организацијата, персоналот и информациските, комуникациските и други електронски ресурси.

ГЛАВА ВТОРА

КЛАСИФИЦИРАЊЕ НА ИНФОРМАЦИИ И СТЕПЕНИ НА КЛАСИФИКАЦИЈА

Член 7

Со класификација на информацијата се определува степенот на заштита на информацијата кој треба да биде соодветен со степенот на штетата што би настанала за Република Македонија со неовластен пристап или неовластена употреба на информацијата.

Информациите кои се предмет на класификација се однесуваат особено на: јавната безбедност; одбраната; надворешните работи; безбедносни, разузнавачки и контраразузнавачки активности на органите на државната управа на Република Македонија; системи, уреди, проекти и планови од важност за јавната безбедност, одбраната, надворешните работи; научни истражувања и технолошки, економски и финансиски работи од значење за Република Македонија.

Член 8

Класификацијата на информациите се врши според нивната содржина.

Степенот на класификација на информацијата го определува создавачот на информацијата, а со негово писмено овластување и друго лице.

Информацијата се означува со еден од степените на класификација:

- ДРЖАВНА ТАЈНА;
- СТРОГО ДОВЕРЛИВО;
- ДОВЕРЛИВО и
- ИНТЕРНО.

Член 9

Класифицираната информација со степен „ДРЖАВНА ТАЈНА“ е информација чие неовластено откривање би предизвикало загрозување и нанесување непоправливи штети на трајните интереси на Република Македонија.

Класифицираната информација со степен „СТРОГО ДОВЕРЛИВО“ е информација создадена од органите на државната управа, органите на единиците на локалната самоуправа, институции и други физички или правни лица, која е од значење за јавната безбедност, одбраната, надворешните работи и безбедносните и разузнавачките активности на органите на државната управа на Република Македонија, а чие неовластено откривање би предизвикало исклучително сериозна штета за виталните интереси на Република Македонија.

Класифицираната информација со степен „ДОВЕРЛИВО“ е информација создадена од органите на државната управа, органите на единиците на локалната самоуправа, институции и други физички или правни лица, која е од значење за јавната безбедност, одбраната, надворешните работи и безбедносните и разузнавачките активности на органите на државната управа на Република Македонија, а чие неовластено откривање би предизвикало сериозна штета за важните интереси на Република Македонија.

Класифицираната информација со степен „ИНТЕРНО“ е информација создадена од органите на државната управа, органите на единиците на локалната самоуправа, институции и други физички или правни лица, чие неовластено откривање би предизвикало штета за работењето на органите на државната управа, единиците на локалната самоуправа, институциите и другите правни лица, кои се од значење за јавната безбедност, одбраната, надворешните работи и безбедносните и разузнавачките активности на органите на државната управа на Република Македонија.

Член 10

При класифицирањето на информацијата, создавачот, односно лицето овластено од него, треба да ја означи класифицираната информација со најсоодветниот степен на класификација со кој ќе се обезбеди потребната заштита на државните интереси и безбедноста.

Определувањето на соодветниот степен на класификација на информацијата ќе се врши врз основа на проценка за можната штета и последици кои би произлегле од неовластениот пристап до неа.

Постапката за класифицирање на информациите поблиску се уредува со правилник донесен од страна на директорот на Дирекцијата.

Член 11

Класифицирана информација со степен „ДРЖАВНА ТАЈНА“ определуваат: претседателот на Република Македонија, претседателот на Собранието на Република Македонија, претседателот на Владата на Република Македонија, претседателот на Уставниот суд на Република Македонија, претседателот на Врховниот суд на Република Македонија, министрите во рамките на своите ресори, јавниот обвинител на Република Македонија, началникот на Генералштабот на Армијата на Република Македонија, директорот на Агенцијата за разузнавање, директорот на Оперативно техничката агенција, директорот на Дирекцијата за безбедност на класифицирани информации, како и лица овластени од страна на горенаведените субјекти.

Ако така е определено со закон, меѓународен договор или друг пропис, класифицирана информација со степен „ДРЖАВНА ТАЈНА“ определуваат и лицата предвидени во тие акти.

Член 12

Информациите со чие откривање би се намалила ефикасноста на работењето на органите на државната управа и институции, добиваат ознака „за ограничена употреба“.

Ознаката „за ограничена употреба“ не претставува степен на класификација, но до ваквите информации не е дозволен слободен пристап.

Начинот на чување и ракување со информациите за ограничена употреба со уредба поблиску ги уредува Владата на Република Македонија.

Член 13

Ако во една информација се опфатени податоци за повеќе степени на класификација, создавачот е должен да го определи степенот на класификација на секој од нив посебно.

Целината на информацијата се класифицира според највисокиот степен на класификација, а на насловната страна на материјалот се означуваат другите делови со степени на класификација коишто припаѓаат кон информацијата.

Ако дел од документот содржи класифицирана информација со повисок степен на класификација, тој дел може да се издвои како посебен документ со соодветен степен на класификација.

Фусните нема да бидат класифицирани освен ако содржат или откриваат класифицирани информации.

Заради избегнување на безбедносен ризик употребата на фусноти треба да се сведе на минимум.

Член 14

Создавачот на класифицираната информација задолжително го означува на видно место степенот на нејзината класификација, согласно овој закон и прописите што произлегуваат од него.

Член 15

Ако информацијата не била означена со степен на класификација, а создавачот не може да се утврди или престанал да постои, класифицирањето на информацијата го врши правниот следбеник на создавачот.

Ако не може да се утврди ниту правниот следбеник, означувањето на степенот на класифицираната информација го врши Дирекцијата.

Член 16

Со рекласификација се врши промена на степенот на класификацијата на информацијата.

Промена на степенот на класификација врши создавачот, а со негово писмено овластување и друго лице.

За промената на степенот на класификација на информацијата задолжително се известуваат корисниците на информацијата.

Начинот на промена на степенот на класификација на информацијата со уредба поблиску го уредува Владата на Република Македонија.

Член 17

Класификацијата на информацијата престанува:

- на датумот означен на документот;
- со случување на определен настан наведен во документот;
- со истекување на временскиот период означен на документот и
- со декласификација.

Член 18

Со декласификација се врши промена од класифицирана информација во информација која е некласифицирана.

Декласификацијата од ставот 1 на овој член ја врши создавачот на информацијата или од него овластено лице за што задолжително ги известува корисниците на информацијата.

Начинот на декласификација на информацијата со уредба поблиску го уредува Владата на Република Македонија.

Член 19

Создавачот на класифицираната информација означува временски период или настан после кој информацијата може да биде рекласифицирана или декласифицирана.

Временскиот период или настанот после кои информацијата може да биде рекласифицирана или декласифицирана не може да надминат период од десет години, освен во случај кога на информацијата ѝ е потребна подолготрајна заштита определена со овој или друг закон.

Член 20

Класифицираната информација со степенот „ДРЖАВНА ТАЈНА“ создавачот ја разгледува и оценува во период не подолг од десет години за да се оцени потребата од натамошно задржување на класификацијата.

Класифицираната информација со степенот „СТРОГО ДОВЕРЛИВО“ се разгледува и оценува во период не подолг од пет години за да се оцени потребата од натамошно задржување на класификацијата.

Класифицираната информација со степенот „ДОВЕРЛИВО“ се разгледува и оценува во период не подолг од три години за да се оцени потребата од натамошно задржување на класификацијата.

Класифицирана информација со степенот „ИНТЕРНО“ се разгледува и оценува во период не подолг од две години за да се оцени потребата од натамошно задржување на класификацијата.

Член 21

Ако со класифицирана информацијата се прикрива пречекорување на овластување, злоупотреба на функцијата или некое друго незаконско дејствие, односно казниво дело, таквата информација нема да се смета за класифицирана.

На лицата кои ќе ја пријават информацијата од став 1 на овој член до надлежен орган согласно Законот за заштита на укажувачите им се гарантира заштита согласно закон.

Класифицирани информации на странски држави и меѓународни организации

Член 22

Класифицираните информации од странски држави или меѓународни организации со кои Република Македонија има склучено меѓународни договори или на кои Република Македонија им пристапила, го задржуваат степенот на класификација што се користи во таа држава или меѓународна организација.

Член 23

Дисеминација на странските класифицирани информации се врши согласно со принципот „потребно е да знае“ и поседување на соодветен безбедносен сертификат.

Пред дисеминацијата на странските класифицирани информации се утврдуваат корисниците и се преземаат активностите за ракување со класифицирани информации.

Начинот на дисеминација на странските класифицирани информации со уредба поблиску го уредува Владата на Република Македонија.

ГЛАВА ТРЕТА

КРИТЕРИУМИ, МЕРКИ И АКТИВНОСТИ ЗА ЗАШТИТА НА КЛАСИФИЦИРАНИ ИНФОРМАЦИИ

Член 24

За заштита на класифицираните информации, се преземаат мерки и активности за административна, физичка, индустриска безбедност, безбедност на комуникациско – информациски системи, како и за безбедност на лица – корисници на класифицирани информации.

Член 25

Критериуми кои особено се земаат предвид при утврдувањето на мерките за заштита на класифицираните информации се:

- степенот на класификација;
- обемот и формата на класифицираната информација и
- процената за закана на безбедноста на класифицираната информација.

Административна безбедност

Член 26

Мерки и активности за административна безбедност се:

- определување на степенот и обележување на класифицираната информација;
- прием и евиденција на класифицираната информација;
- определување начин за чување, ракување и контрола на класифицираната информација;
- репродукција, преводи и извадоци на класифицираната информација и одредување на бројот на примероците и корисниците;
- дисеминација на класифицирани информации;
- пренос на класифицирани информации,
- отстранување и уништување на класифицираната информација.

Мерките и активностите за административна безбедност со уредба поблиску ги уредува Владата на Република Македонија.

Физичка безбедност

Член 27

Физичката безбедност се остварува со примена на физички и технички заштитни мерки со цел да се спречи неовластен пристап до класифицирани информации.

Мерките за физичка безбедност треба да спречат прикриен или насилен упад од неовластено лице, да одвратат, спречат и детектираат неовластени активности воопшто, како и да овозможат поделба на персоналот во нивниот пристап до класифицирани информации согласно принципот „потребно е да знае“.

Мерките за физичка безбедност се применуваат во објекти, згради, канцеларии, простории и други места во кои се ракува, се чуваат или електронски се обработуваат класифицирани информации.

Просториите во кои се чуваат класифицирани информации со степен „ДОВЕРЛИВО“ и повисоко, ќе се воспостават како безбедносни зони.

За заштита на класифицирани информации со степен „ДОВЕРЛИВО“ и повисоко се користи опрема, системи или други технички средства кои исполнуваат минимални стандарди поблиску уредени со подзаконски акт што го донесува директорот на Дирекцијата.

Член 28

Мерки и активности за физичка безбедност се:

- процена за можно нарушување на безбедноста на класифицираната информација;
- определување на безбедносен појас околу објектот;
- определување на безбедносни и административни зони;
- организирање на физичка заштита и примена на технички средства за обезбедување на објекти и простории во кои се наоѓаат класифицирани информации;
- контрола на влез, движење и излез на лица и возила за пренос на класифицирани информации и
- обезбедување при пренос на класифицирани информации надвор од безбедносните зони.

Мерките и активностите за физичка безбедност со уредба поблиску ги уредува Владата на Република Македонија.

Безбедност на лица – корисници на класифицирани информации

Член 29

Мерки и активности за безбедност на лица – корисници на класифицирани информации се:

- определување на офицер за безбедност на класифицирани информации;
- безбедносна проверка;
- издавање на безбедносен сертификат;
- издавање на дозвола за пристап до класифицирани информации и
- проверка и оценување на способноста за постапување со класифицирани информации.

Мерките и активностите за безбедност на лица корисници на класифицирани информации со уредба поблиску ги уредува Владата на Република Македонија.

Безбедност на комуникациско-информациски системи

Член 30

Безбедност на комуникациско-информациски системи (КИС) е примена на безбедносни мерки за заштита на комуникациските, информациските и другите електронски системи, и на класифицираните информации кои се создаваат, чуваат, обработуваат или пренесуваат во овие системи со цел да се обезбеди нивна доверливост, интегритет, достапност, автентичност и неотповикливост.

Заради обезбедување на целите од став 1 на овој член се имплементира соодветен систем на безбедносни мерки (физичка, безбедност на лица - корисници на класифицирани информации, административна и безбедност на КИС) со цел создавање на безбедносна околина во која ќе функционираат комуникациските, информациските или другите електронски системи.

Соодветниот систем на безбедносни мерки на КИС треба да се заснова врз процес за управување со ризик.

Член 31

Мерки и активности за безбедност на комуникациско-информациски системи се:

- акредитација на комуникациско-информациски системи и процеси;
- процена за можно нарушување на безбедноста на класифицираната информација со неовластено навлегување во КИС во кој се чуваат и обработуваат класифицирани информации;
- утврдување на методи и безбедносни процедури за прием, обработка, пренос, чување и архивирање на класифицирани информации во електронска форма;
- заштита при создавање, чување, обработка или пренос на класифицирани информации во комуникациско-информациски системи;

- криптографска безбедност на комуникациски, информациски и други електронски системи преку кои се создаваат, чуваат, обработуваат и пренесуваат класифицирани информации;
- заштита од компромитирачко електромагнетно зрачење;
- определување на зони и простории заштитени од компромитирачко електромагнетно зрачење и
- инсталирање на уреди за чување на класифицирани информации.

Мерките и активностите за безбедност на комуникациско-информациски системи со уредба поблиску ги уредува Владата на Република Македонија.

Член 32

Мерки и активности за криптографска безбедност се:

- евалуација и одобрување на криптографски материјали и производи;
- развој на криптографски алгоритми и производи;
- управување со криптографски материјали;
- примена на соодветни мерки и процедури за евиденција, безбедно ракување, чување и дистрибуција на криптографски материјали и производи;
- обука на лица за работа со криптографски материјали и производи
- контрола на горенаведените мерки, процедури и на начинот на употреба на криптографските материјали и производи;

Мерките и активностите за криптографска безбедност со уредба поблиску ги уредува Владата на Република Македонија.

Член 33

Пренос на класифицирани информации преку комуникациски системи надвор од безбедносните зони се врши исклучиво со примена на криптографска заштита.

За пренос на класифицирани информации од став 1 на овој член, се користат само криптографски производи одобрени од Националниот совет за ИКТ.

По исклучок од став 1 на овој член, може да се применат посебни процедури во случај на воена, вонредна или кризна состојба во Република Македонија или во специфични технички конфигурации со уредба поблиску ги утврдува Владата на Република Македонија.

Индустриска безбедност

Член 34

Мерките за индустриска безбедност се применуваат со цел обезбедување заштита на класифицираните информации од страна на договарачите и сите субјекти

вклучени во преговорите пред склучување на договор и во текот на реализација на класифицираниот договор.

Мерките треба да обезбедат заштита на класифицираните информации при транспорт и при воспоставување на процедури за посета на физички и правни лица од други земји на објекти каде што се ракува со класифицирани информации.

За пристап и ракување со класифицирани информации при реализирање на класифицирани договори, транспорт и посети на објекти каде што се ракува со класифицирани информации, физичките и правните лица треба да поседуваат соодветен безбедносен сертификат.

Мерките и активностите за индустриска безбедност со уредба поблиску ги уредува Владата на Република Македонија.

Размена на класифицирани информации со странски држави и меѓународни организации

Член 35

Класифицирана информација на странска држава или меѓународна организација е информација којашто надлежниот орган на странската држава или меѓународната организација ја отстапил на Република Македонија со обврска да се обезбеди неговата заштита.

Со класифицираните информации примени од странска држава или меѓународна организација се постапува на начин којшто е предвиден со меѓународен договор.

Ако меѓународниот договор од ставот 2 на овој член не содржи одредби за начинот на постапување со класифицираните информации, се постапува согласно со одредбите на овој закон.

Член 36

Во случај на воена, вонредна или кризна состојба во Република Македонија, по барање на надлежните органи согласно со Уставот и законите, Дирекцијата може да врши размена на класифицирани информации со странски држави и меѓународни организации со кои не се склучени меѓународни договори по претходна согласност од страна на Владата, ако е тоа во интерес на Република Македонија

По завршување на воената, вонредната или кризната состојба од став 1 на овој член, Дирекцијата ќе достави извештај до Владата за разменетите класифицирани информации со странски држави и меѓународни организации со кои не се склучени меѓународни договори.

Член 37

Во согласност со преземените обврски од ратификуваните меѓународни договори, Дирекцијата овозможува вршење контрола на овластени претставници на странски држави и меѓународни организации, на начинот на користење и заштита на класифицираните информации што од нив се отстапени на користење во Република Македонија.

Контрола на начинот на користење и заштита на доставените класифицирани информации од Република Македонија до странските држави и меѓународните организации врши Дирекцијата согласно со овој закон и меѓународните договори.

Користење на класифицирани информации

Член 38

Орган на државната управа, институција или физичко или правно лице во Република Македонија кое има безбедносен сертификат или странски државен орган, институција или странско физичко или правно лице кое има безбедносен сертификат на матичната држава и дозвола за пристап до класифицирани информации издадена од Дирекцијата, може да биде корисник на класифицирани информации согласно принципот „потребно е да знае“.

Член 39

За извршување на работните задачи, на лицата во органите на државната управа, органите на единицата на локалната самоуправа, институциите, јавните претпријатија, јавните установи и служби, како и други правни и физички лица им се издава безбедносен сертификат согласно со принципот „потребно е да знае“.

Безбедносен сертификат се издава за пристап до соодветен степен на класифицирани информации.

За издавање на безбедносен сертификат за пристап до соодветен степен на класифицирани информации, заинтересираното физичко или правно лице поднесува писмено барање до Дирекцијата.

Барањето за издавање на безбедносен сертификат од став 3 на овој член се поднесува преку офицер за безбедност на класифицирани информации во правното лице.

Постапката за издавање на безбедносен сертификат за лицата вработени во Дирекцијата се спроведува преку офицерот за безбедност на класифицирани информации во Дирекцијата.

Безбедносен сертификат од ставот 2 на овој член издава директорот на Дирекцијата за безбедност за класифицирани информации врз основа на претходно спроведена безбедносна проверка и оценка за постоење или непостоење на безбедносен ризик за ракување со класифицирани информации.

Член 40

Безбедносен сертификат за пристап и користење на класифицирани информации од сите степени, без претходна безбедносна проверка, заради непречено вршење на функцијата од денот на изборот до крајот на мандатот, добиваат: претседателот на Република Македонија, претседателот на Собранието на Република Македонија, претседателот на Владата на Република Македонија, заменик на претседателот на Владата на Република Македонија, претседателот на Уставниот суд

на Република Македонија и претседателот на Врховниот суд на Република Македонија.

Член 41

Безбедносен сертификат се издава на физичко лице кое ги исполнува следниве услови:

- да е државјанин на Република Македонија;
- да постои оправдана потреба за користење на класифицирани информации согласно со принципот „потребно е да знае“;
- да не постојат безбедносни пречки за пристап и ракување со класифицирани информации што се утврдува со оперативна проверка;
- физичкото лице да има деловна способност;
- лицето да наполнило 18 години, а за користење на класифицирани информации означени со степен „ДРЖАВНА ТАЈНА“ да наполнило 21 година;
- да не му е изречена санкција забрана за вршење на професија, дејност или должност;
- да е обучено за ракување со класифицирани информации;
- од оперативната проверка за лицата наведени во безбедносниот прашалник да не произлегува постоење на безбедносни пречки за пристап и ракување со класифицирани информации.

Член 42

Безбедносен сертификат се издава на правно лице кое ги исполнува следниве услови:

- а е регистрирано во Република Македонија; Д
- а постои оправдана потреба за пристап и ракување со класифицирани информации согласно принципот „потребно е да знае“; Д
- а не му е изречена санкција – забрана за вршење на дејност; Д
- да има обезбедено услови за физичка, административна и/или безбедност на компјутерско-информациски системи, доколку тоа го бараат условите од класифицираниот договор;
- да има обезбедено безбедносни сертификати за овластените лица во правното лице;
- да е финансиски и економски стабилно и
- да не постојат безбедносни пречки за ракување со класифицирани информации што се утврдува со оперативна проверка.

Член 43

Правното лице ќе се смета за способно да обезбеди заштита на класифицирани информации доколку обезбеди услови за спроведување на мерките и активностите за заштита на класифицирани информации определени со овој закон.

Утврдувањето на финансиската и економската стабилност на правното лице и постапката за издавање безбедносен сертификат за правно лице со уредба поблиску ги уредува Владата на Република Македонија.

Постапки за издавање на безбедносни сертификати

Член 44

Исполнувањето на условите за издавање на безбедносен сертификат се утврдува преку безбедносна проверка.

Безбедносната проверка од ставот 1 на овој член се врши врз основа на претходна писмена согласност од физичкото или правното лице кое поднело барање за издавање на безбедносниот сертификат, којашто е составен дел на барањето од членот 39 став 3 на овој закон.

Ако физичкото или правното лице во текот на постапката писмено ја повлече својата согласност за проверка, повторна постапка за безбедносна проверка не може да се спроведе пред истекот на една година од денот на повлекувањето на согласноста.

Член 45

Безбедносна проверка се спроведува пред издавање на безбедносен сертификат на правни и физички лица за пристап и ракување на класифицирани информации, со цел да се утврди постоење или непостоење на безбедносен ризик.

Безбедносната проверка започнува по поднесување на барањето до Дирекцијата.

Пополнетите податоци од безбедносниот прашалник претставуваат дел од содржината на безбедносната проверка.

Формата и содржината на обрасците на безбедносниот прашалник од ставот 1 на овој член со правилник ги пропишува директорот на Дирекцијата.

Член 46

Пополнетиот прашалник за безбедносна проверка се класифицира со степенот „ИНТЕРНО“.

Податоците од пополнетиот безбедносен прашалник од ставот 1 на овој член се користат за целите на проверката.

Член 47

За користење на класифицирани информации означени со степенот „ИНТЕРНО“ не се врши безбедносна проверка и не се издава безбедносен сертификат.

Физичкото или одговорното лице во правното лице се информира за обврската за заштита на класифицираните информации што му се дадени на увид, односно ракување.

Член 48

Во зависност од степенот на класифицираната информација за која е поднесено барање за издавање безбедносен сертификат за физичко лице, се врши безбедносна проверка соодветна на степенот на класифицираната информација и тоа:

- а) од прв степен за информација класифицирана „ДОВЕРЛИВО“;
- б) од втор степен за информација класифицирана „СТРОГО ДОВЕРЛИВО“ и
- в) од трет степен за информација класифицирана „ДРЖАВНА ТАЈНА“.

Член 49

Со безбедносна проверка од прв степен се проверува:

- идентитетот на лицето (врз основа на приложена писмена документација) и оперативната проверка на податоците за лицето од надлежен орган;
- возраста од минимум 18 години;
- државјанството на Република Македонија;
- деловната способност на лицето (врз основа на уверение од надлежен орган) и
- постоење на безбедносни пречки за пристап и ракување со класифицирани информации кај лицето (утврдени со спроведување на оперативна проверка од страна на надлежен орган).

Член 50

Со безбедносна проверка од втор степен се проверува :

- идентитетот на лицето (врз основа на приложена писмена документација, и оперативна проверка на податоците за лицето од страна на надлежен орган);
- возраста од минимум 18 години;
- државјанството на Република Македонија;
- деловната способност на лицето (врз основа на уверение од надлежен орган) и
- постоењето на безбедносни пречки за пристап и ракување со класифицирани информации кај лицето – барател на безбедносен

сертификат и кај лицата наведени во безбедносниот прашалник (со спроведување на оперативната проверка од страна на надлежен орган).

Член 51

Со безбедносна проверка од трет степен се проверува :

- идентитетот на лицето (врз основа на приложена писмена документација, и оперативна проверка на податоците за лицето од страна на надлежен орган); И
- возраста од минимум 21 година; В
- државјанството на Република Македонија; Д
- теловната способност на лицето (врз основа на уверение од надлежен орган) Д
и
- постоењето на безбедносни пречки за пристап и ракување со класифицирани информации кај лицето барател на безбедносен сертификат и кај лицата наведени во безбедносниот прашалник (со спроведување на оперативната проверка од страна на надлежен орган).

Член 52

На барање на Дирекцијата, оперативните проверки за постоење на безбедносни пречки за пристап и ракување со класифицирани информации ги вршат:

- надлежните служби на Министерството за внатрешни работи за сите физички и правни лица, освен за лицата утврдени во алинејата 2 на овој член и
- надлежните служби на Министерството за одбрана за сите вработени во Министерството за одбрана и Армијата на Република Македонија.

Во вршењето на безбедносните проверки, по потреба Дирекцијата соработува и со други органи на државната управа и институции.

Член 53

Постапката за спроведување на безбедносна проверка трае најмногу до:

- два месеци за безбедносната проверка од прв степен за физички лица;
- четири месеци за безбедносната проверка од втор степен за физички лица
- шест месеци за безбедносната проверка од трет степен за физички лица и
- шест месеци за безбедносна проверка за правно лице.

По исклучок од ставот 1 на овој член, постапката за безбедносна проверка од трет степен за лицата назначени во надзорните тела кои вршат надзор над спроведувањето на мерките за следење на комуникациите, како и за ангажираните акредитирани национални и меѓународни технички експерти од тие тела, согласно со Законот за следење на комуникациите, трае еден месец од денот на поднесување на барањето.

По исклучок од ставот 1 на овој член, постапката за безбедносна проверка од втор степен за лицата пред засновање на работен однос во Оперативно-техничката агенција, согласно со Законот за Оперативно-техничка агенција, трае еден месец од денот на поднесување на барањето.

Во посложени случаи, роковите од ставот 1 на овој член може да бидат двојно продолжени.

Времетраење на безбедносните сертификати

Член 54

Безбедносниот сертификат издаден за информација класифицирана со степен „ДРЖАВНА ТАЈНА“ важи пет години.

Безбедносниот сертификат издаден за информација класифицирана со степен „СТРОГО ДОВЕРЛИВО“ важи десет години.

Безбедносниот сертификат издаден за информација класифицирана со степен „ДОВЕРЛИВО“ важи десет години.

Безбедносниот сертификат започнува да важи од денот на завршување на безбедносната проверка и оцената на безбедносниот ризик.

Содржината и формата на образецот на безбедносните сертификати од ставовите 1, 2 и 3 на овој член со правилник ги пропишува директорот на Дирекцијата.

Член 55

Корисникот на класифицирани информации е должен да поднесе ново барање за продолжување на важноста на безбедносниот сертификат најдоцна шест месеци пред денот на истекот на неговата важност.

За физичкото и правното лице кое поднесува барање за продолжување на важноста на безбедносниот сертификат, се врши повторна безбедносна проверка согласно овој закон соодветна на степенот на класифицираните информации што му се отстапуваат на користење.

Член 56

Ако се утврди дека физичкото или правното лице не постапува со класифицираните информации согласно со овој закон или повеќе не е исполнет некој од условите врз основа на кои е издаден безбедносниот сертификат, директорот на

Дирекцијата донесува решение за одземање на безбедносниот сертификат и пред истекот на неговото важење.

Во решението од ставот 1 на овој член не се дава образложение за причините за престанокот на важноста на безбедносниот сертификат.

Против решението од став 1 на овој член за одземање на безбедносниот сертификат и пред истекот на неговата важност лицето има право на жалба до Државната комисија за одлучување во управна постапка и постапка од работен однос во втор степен.

Член 57

Директорот на Дирекцијата може да донесе решение за одбивање на барањето за издавање на безбедносен сертификат за физички и правни лица ако не се исполнети условите од овој закон.

Во решението од ставот 1 на овој член не се дава образложение за причините за одбивање на барањето за издавање на безбедносен сертификат.

Против решението од ставот 1 на овој член лицето чие барање е одбиено може да поднесе жалба до Државната комисија за одлучување во управна постапка и постапка од работен однос во втор степен.

Член 58

Жалбата од членот 56 и 57 на овој закон се поднесува во рок од 15 дена од денот на приемот на решението, до Државната комисија за одлучување во управна постапка и постапка од работен однос во втор степен.

Решението од ставот 1 на овој член донесено од Комисијата е конечно.

Член 59

Барање за повторно издавање на безбедносен сертификат со ист или повисок степен може да се поднесе:

- по истекот на една година од правосилноста или конечноста на решението за одбивање на барањето за издавање на безбедносен сертификат и
- по истекот на три години од правосилноста или конечноста на решението за одземање на безбедносниот сертификат пред истекот на важноста.

Член 60

Безбедносниот сертификат престанува да важи со истекот на рокот на неговата важност, како и во случај на:

- престанок на функцијата на лицата од членот 40 на овој закон;
- престанок на потребата за пристап до класифицирани информации согласно со принципот „потребно е да знае“ или
- смрт на физичкото лице или престанок на правното лице.

Со престанок на важноста во случаите од став 1 на овој член, безбедносниот сертификат се враќа кај офицерот за безбедност, а во случај на престанок на правното лице безбедносниот сертификат се враќа во Дирекцијата.

Член 61

Дозволата за пристап до класифицирани информации престанува да важи:

- со истекот на рокот на важноста наведен во дозволата;
- со извршување на задачата за која била издадена;
- ако потребата од издавањето на дозволата престанала да постои или е изменета и
- ако се утврди дека правното и физичкото лице не постапуваат со класифицираните информации согласно закон.

Член 62

Обврската за заштита на тајноста на класифицираните информации продолжува и по истекот на важноста на безбедносниот сертификат.

Член 63

За потребите на судска постапка или постапка пред друг надлежен орган во која ќе се користат класифицирани информации, субјектите во постапката е потребно да поседуваат безбедносен сертификат.

Постапката ќе се води во присуство на лицето за чиешто права, обврски или одговорност се одлучува во нејзини рамки, дури и кога лицето нема безбедносен сертификат.

Лицето од став 2 на овој член е одговорно за исполнување на обврската за заштита на класифицираните информации согласно член 2 од овој закон и други релевантни одредби, а во спротивно ќе одговара согласно со закон.

Јавноста, во соодветната постапка, ќе биде исклучена.

За користење на класифицирана информација во постапка пред надлежен орган, соодветниот орган треба да го информира создавачот на класифицираната информација, освен ако создавачот не ја достави на користење во постапката, како и Дирекцијата.

Член 64

Дирекцијата води евиденција за издадените безбедносни сертификати и за пополнетите безбедносни прашалници.

Дирекцијата води посебна евиденција за издадените дозволи за пристап до класифицирани информации во Република Македонија.

Содржината, формата и начинот на водење на евиденциите од ставовите 1 и 2 на овој член, со правилник ги пропишува директорот на Дирекцијата.

ГЛАВА ЧЕТВРТА

ОРГАНИ ЗА ЗАШТИТА НА КЛАСИФИЦИРАНИ ИНФОРМАЦИИ

Офицер за безбедност на класифицирани информации

Член 65

Органите на државната управа, органите на локалната самоуправа, институциите, јавните претпријатија и установи и други правни лица, се должни да создадат услови неопходни за заштита на класифицирани информации и да преземат мерки за елиминирање на негативните последици ако дојде до откривање на класифицираните информации.

За ефикасно и координирано извршување на правата и обврските кои се однесуваат на класифицираните информации, во субјектите од ставот 1 на овој член се определува офицер за безбедност на класифицирани информации.

Член 66

Одговорното лице во субјектите од член 65 став 1 определува еден или повеќе офицери за безбедност на класифицирани информации, во зависност од бројот и обемот на класифицираните информации во субјектот.

По исклучок, во зависност од бројот и обемот на класифицирани информации, одговорното лице во субјектот може и да ја извршува должноста на офицер за безбедност на класифицирани информации.

Офицерот за безбедност на класифицирани информации изготвува и поднесува квартални извештаи за состојбата со класифицираните информации во субјектот директно до одговорното лице, по исклучок на став 2 од овој член.

Доколку во субјектот се определени повеќе офицери за безбедност на класифицирани информации, одговорното лице определува еден од нив за координација со Дирекцијата.

Член 67

Офицерот за безбедност на класифицирани информации може да биде назначен доколку ги исполнува следните услови:

- а е државјанин на Република Македонија, но не и на друга држава; Д
- а му е одобрен пристап до соодветно ниво на класифицирани информации според условите и постапката утврдени со закон; Д

- а има поминато обука за офицер за безбедност на класифицирани информации; Д
- ицето од ставот 2 на член 65 треба да поседува соодветен безбедносен сертификат. Л

Член 68

Офицерот за безбедност на класифицирани информации е должен:

- а се грижи за спроведување на одредбите на овој закон и на меѓународните договори во врска со безбедноста на класифицираните информации во субјектот; Д
- ериодично да ги проверува евиденциите и протокот на материјалите и документите; П
- а се грижи за правилно и навремено спроведување на архивирањето и ништењето на класифицирани информации; Д
- а ја спроведе постапката за доставување барања за издавање на безбедносен сертификат во рамките на субјектот и да го ажурира регистарот на лица за кои е спроведена постапка; Д
- а ја извести Дирекцијата за истекот на безбедносните сертификати, престанок на работењето или преместување на корисниците на класифицирани информации; Д
- а ја извести Дирекцијата за потребата за промена на степенот на безбедносниот сертификат; Д
- а ја известува Дирекцијата, во писмена форма за секоја промена на податоците во безбедносниот прашалник или промена на условите за добивање на безбедносен сертификат; Д
- а ги евидентира случаите на неовластен пристап до класифицирани информации и на преземени дејствија и веднаш да ја извести Дирекцијата за таков случај и дејствие; Д
- а ги информира корисниците на класифицирани информации најмалку еднаш годишно за правата и обврските при ракување со класифицирани информации; Д

- а обезбедува стручна помош при класификацијата на информацијата во субјектот;

Д

- а организира обука за корисниците на класифицирани информации во субјектот за заштита на класифицирани информации.

Д

За надлежностите определени во став 1 од овој член, офицерот за безбедност изработува годишен план.

Дирекција за безбедност на класифицирани информации

Член 69

Дирекцијата е самостоен орган на државната управа со својство на правно лице.

Дирекцијата:

- обезбедува континуирано спроведување на меѓународните стандарди и нормативи во преземањето на мерките и активностите за заштита на класифицираните информации;
- врши координација на активностите во обезбедувањето заштита на класифицираните информации со државните органи и институциите кои вршат размена на класифицирани информации со странски држави и меѓународни организации;
- ги подготвува, организира, спроведува и го следи спроведувањето на мерките и активностите за обезбедување заштита на класифицирани информации кои на Република Македонија и се отстапени на користење од странски држави и меѓународни организации;
- презема активности за заштита на класифицирани информации отстапени од Република Македонија на странски држави и меѓународни организации;
- учествува во изготвување на планови и програми на Република Македонија за членство во меѓународни организации од областа за обезбедување заштита на класифицираните информации;
- планира и остварува меѓународна соработка за заштита и размена на класифицираните информации;
- предлага мерки за унапредување на заштитата на класифицирани информации;
- покренува иницијативи за склучување меѓународни договори со странски држави и меѓународни организации од областа на размената на класифицирани информации;
- организира и спроведува обуки за безбедност на класифицирани информации;
- врши инспекциски надзор над спроведувањето на одредбите на овој закон и другите прописи од областа на класифицираните информации, и
- врши други работи утврдени со овој и друг закон.

За своето работење Дирекцијата донесува годишен план, а подготвува и извештај кои ги усвојува Владата на Република Македонија.

Член 70

Во размената и заштитата на класифицирани информации со НАТО и со ЕУ, Дирекцијата ги врши задачите на безбедносно тело за:

- координација и спроведување на безбедносните политики на НАТО и на ЕУ во Република Македонија, со цел обезбедување соодветно ниво на заштита на класифицираните информации во согласност со склучените договори;
- безбедност во комуникација за избор, управување и одржување на криптографската опрема за пренос, обработка и чување на класифицираните податоци;
- спроведување безбедносна акредитација на КИС и процесите во кои се користат класифицирани информации;
- управување со материјали за криптографска заштита на класифицирани информации и безбедно ракување, чување, дистрибуција и евиденција на криптоматеријалите;
- преземање мерки и активности за заштита на КИС од компромитирачко електромагнетно зрачење.

Регистри и контролни точки

Член 71

За вршење на работи од надлежност на Дирекцијата со НАТО класифицирани информации, ЕУ класифицирани информации и други странски класифицирани информации се воспоставуваат регистар, подрегистри и контролни точки.

Регистарот за НАТО класифицирани информации, ЕУ класифицирани информации и други странски класифицирани информации се води во Дирекцијата, а подрегистри и контролни точки се водат во министерствата, други органи на државната управа, институции и правни лица во коишто се ракува и се чуваат НАТО класифицирани информации, ЕУ класифицирани информации и други странски класифицирани информации.

Од подрегистрите и контролните точки од ставот 1 на овој член се доставуваат информации потребни за извршување на работите на Дирекцијата и се врши размена на класифицирани информации со странство.

Бројот на подрегистрите и контролните точки, на предлог на Дирекцијата, со одлука го определува Владата на Република Македонија.

Размената на класифицирани информации од Република Македонија со странски држави и меѓународни организации се врши преку Дирекцијата, ако со друг закон или меѓународен договор поинаку не е уредено.

Член 72

Дирекцијата ги известува надлежните органи на странските држави и меѓународни организации за безбедноста на разменетите класифицирани информации и од нив прима известувања за безбедноста на класифицираните информации кои им се отстапени од Република Македонија, согласно важечките меѓународни договори.

Член 73

На барање на Дирекцијата, органите на државната управа, органите на единиците на локалната самоуправа, институциите и други правни и физички лица ѝ даваат информации кои се потребни за извршување на работите од нејзина надлежност.

Член 74

Со Дирекцијата за безбедност на класифицирани информации раководи директор кој го именува и разрешува Владата на Република Македонија.

Директорот се именува со мандат од четири години.

За именување на директор се објавува јавен оглас во три дневни весници кои се издаваат на целата територија на Република Македонија од кои еден се издава на јазикот што го зборуваат најмалку 20% од граѓаните кои зборуваат службен јазик различен од македонскиот јазик.

За директор на Дирекцијата може да биде именувано лице кое ги исполнува следниве услови:

- 1) да е државјанин на Република Македонија;
- 2) да не му е изречена казна забрана за вршење на професија, дејност или должност, со правосилна одлука;
- 3) да има стекнати 240 кредити според ЕКТС или VII/1 степен на образование,
- 4) да има најмалку пет години работно искуство;
- 5) да поседува еден од следниве меѓународно признати сертификати или уверенија за активно познавање на англискиот јазик не постар од пет години:
 - ТОЕФЕЛ ИБТ најмалку 74 бода,
 - ИЕЛТС (IELTS) - најмалку 6 бода,
 - ИЛЕЦ (ILEC) (Cambridge English: Legal) - најмалку Б2 (B2) ниво,
 - ФЦЕ (FCE) (Cambridge English: First) - положен,
 - БУЛАТС (BULATS) - најмалку 60 бода и
 - АПТИС (APTIS) - најмалку ниво Б2 (B2) и
- 6) поседува потврда за положен психолошки тест и тест за интегритет.

Функцијата директор престанува поради следниве основи:

- на негово барање;
- ако трајно ја загуби способноста за вршење на функцијата;
- ако ги исполни условите за старосна пензија согласно со закон;
- ако е осуден со правосилна судска пресуда за кривично дело на безусловна казна затвор во траење од најмалку шест месеци;
- кога ќе престане да го исполнува условот наведен во ставот 4 алинеја 2 на овој член и
- поради нестручно и несовесно работење.

Член 75

Вработените во Дирекцијата се административни службеници. Во однос на нивните права и одговорности од работен однос се применуваат одредбите од Законот за административни службеници.

Вработените во Дирекцијата треба да поседуваат соодветен безбедносен сертификат за пристап до класифицирани информации. Степенот на безбедносниот сертификат се утврдува со правилникот за систематизација на работните места во Дирекцијата.

Вработените во Дирекцијата имаат легитимација која ја издава директорот на Дирекцијата.

Образецот на легитимацијата и постапката за нејзино издавање со правилник ги пропишува директорот на Дирекцијата.

ГЛАВА ПЕТТА

ПЛАНОВИ И ПРОГРАМИ ЗА РАБОТЕЊЕ НА ДИРЕКЦИЈАТА И ФИНАНСИРАЊЕ НА ДИРЕКЦИЈАТА

Член 76

Работата на Дирекцијата се води и реализира според принципите, нормите и процедурите кои важат во системот на планирањето, програмирањето и буџетското работење.

Член 77

Финансиските средства за потребите на Дирекцијата се обезбедуваат од Буџетот на Република Македонија.

Финансиските средства за потребите на Дирекцијата можат да се обезбедат и од други извори, во согласност со закон.

Финансиските средства за органите на државната управа за потребите на заштитата, користењето и меѓународната размена на класифицираните информации се

обезбедуваат од Буџетот на Република Македонија во рамките на финансиските средства на тие органи.

Јавните претпријатија, институциите и службите од посебно значење за заштитата, користењето и меѓународната размена на класифицираните информации обезбедуваат финансиски средства од сопствени извори и од финансиски и материјални средства на Република Македонија.

ГЛАВА ШЕСТА

НАДЗОР

Член 78

Инспекциски надзор над спроведувањето на овој закон и прописите донесени врз основа на овој закон врши Дирекцијата преку инспекторите за безбедност на класифицирани информации (во натамошниот текст: инспектори).

Работите на инспекцискиот надзор во рамките на Дирекцијата се вршат во посебна организациона единица.

Член 79

Во постапката за вршење на инспекциски надзор ќе се применуваат одредбите од Законот за инспекциски надзор и Законот за општата управна постапка доколку со овој закон не е поинаку уредено.

Член 80

Инспекторот, кој го врши инспекцискиот надзор покрај општите услови утврдени со Законот за инспекциски надзор потребно е да ги исполнува следниве посебни услови:

- а има стекнато 240 кредити според ЕКТС, или завршен VII/1 степен; Д
- а има 5 години работно искуство во областа на безбедноста на класифицирани информации; Д
- а има лиценца за инспектор од областа на надлежноста на инспекциската служба. Д

Член 81

Инспекторот врши инспекциски надзор во органите на државната управа, јавните претпријатија, институциите и службите од значење за заштитата, користењето и меѓународната размена на класифицираните информации, како и други правни и физички лица.

Во извршувањето на работата инспекторот е самостоен во својата работа.

Инспекторите се должни да постапуваат согласно законот и прописите.

Инспекторите треба да обезбедуваат објективна примена на законот.

Член 82

Во вршењето на инспекцискиот надзор од членот 78 на овој закон, инспекторите се овластени:

- а вршат надзор над спроведувањето на овој закон и другите прописи од областа на безбедноста на класифицираните информации, Д
- а предлагаат мерки за отстранување на утврдените неправилности и недостатоци во определен рок и Д
- а преземаат други дејствија согласно закон. Д

Член 83

Службеното својство на инспекторот се докажува со легитимација.

При вршењето на инспекцискиот надзор, инспекторите се должни да се легитимираат.

Легитимацијата од ставот 1 на овој член ја издава и одзема директорот на Дирекцијата.

Образецот, формата и содржината на легитимацијата, како и начинот и постапката за нејзино издавање и одземање, со правилник ги пропишува директорот на Дирекцијата.

Член 84

Заради вршење на инспекциски надзор, органите на државната управа, јавните претпријатија, институциите и службите од посебно значење за заштитата, користењето и меѓународната размена на класифицираните информации, како и други правни и физички лица се должни да овозможат непречено вршење на надзорот од областа на безбедноста на класифицираните информации.

Инспекцискиот надзор може да биде редовен, вонреден или контролен.

Редовниот инспекциски надзор опфаќа надзор над спроведувањето на овој закон и се врши според Годишна програма и квартални планови што директорот на Дирекцијата ги донесува во согласност со закон.

Вонредниот надзор се врши врз основа на иницијатива поднесена од органи на државната управа, институции, физички или правни лица, како и во случај на сомневање на инспекторот (по службена должност).

Контролниот инспекциски надзор се врши по истекот на рокот определен во решението за отстранување на утврдени недостатоци.

При вршењето на инспекцискиот надзор, инспекторите имаат право на пристап и увид во секое време и без најава, во објекти, деловни простории, станбени простории и во простории во кои се ракува и се чуваат класифицирани информации.

За вршење на работите од ставот 6 на овој член во станбени простории, инспекторите се должни да обезбедат судски налог.

При вршењето на инспекцискиот надзор, инспекторите може да побараат присуство на овластено лице од органот на државната управа надлежен за вршење на работите од областа на полициските работи, заради нивна заштита.

Член 85

Ако при вршењето на инспекцискиот надзор, инспекторот утврди недостатоци и неправилности во врска со исполнетоста на условите за безбедност на класифицираните информации, ќе донесе решение со кое ќе нареди отстранување на утврдените недостатоци и неправилности во определен рок.

Против решението на инспекторот од ставот 1 на овој член, може да се поднесе жалба во рок од осум дена од денот на приемот на решението.

По жалбата на решението на инспекторот одлучува Државната комисија за одлучување во втор степен од областа на инспекцискиот надзор и прекршочната постапка.

Член 86

За извршениот инспекциски надзор, инспекторот составува записник со наод на состојбата кој ќе го достави на начин и во рок предвиден со закон.

Во записникот од ставот 1 на овој член се внесува констатираната состојба и предложените мерки и рокови за отстранување на недостатоците и неправилностите. Одговорното лице во субјектот на надзорот е должно да постапи според записникот и да го извести инспекторот за преземените активности.

Член 87

Ако инспекторот утврди дека во употреба се наоѓаат уреди, технички средства, инсталации и системи кои не одговараат на пропишаните безбедносни стандарди и критериуми за заштита на класифицирани информации, со решение ќе изрече забрана на нивна употреба и нивно отстранување.

Член 88

Ако инспекторот при вршењето на надзорот утврди дека постои непосредна опасност од нарушување на безбедноста на објектите или просториите, документите, опремата, системите и лицата во безбедносниот појас, безбедносната зона или административната зона, со решение ќе изрече забрана за користење на просторот, објектот или дел од објектот.

Член 89

Заради извршувањето на решението од членовите 85 и 87 на овој закон, инспекторот ќе изврши запечатување на предметниот објект или простории.

Запечатувањето од ставот 1 на овој член се означува со жиг на Дирекцијата.

Содржината и формата на жигот, како и начинот на запечатување, со правилник ги пропишува директорот на Дирекцијата.

Член 90

По отстранување на утврдените недостатоци, поради кои е изречена мерката забрана, а по писмено барање на субјектот на кој му е изречена мерката, инспекторот ќе изврши отпечатување.

Член 91

Во вршењето на надзорот во примената на одредбите на овој закон и другите прописи од областа на безбедноста на класифицираните информации, инспекторите можат да наредат преземање на следниве мерки:

- демонтирање, преместување или отстранување на опрема, уреди, инсталации и системи со кои се загрозува безбедноста на класифицираните информации;
- определување на безбедносен појас, безбедносни зони и административни зони околу објектот, просторот или просторијата во објектот во кој се ракува или се чуваат класифицирани информации;
- поставување на безбедносна информатичко-комуникациска опрема, системи и инсталации за безбедност на класифицираните информации;
- преместување или отстранување на лица без соодветен безбедносен сертификат или без соодветна дозвола за пристап во безбедносен појас околу објектот и од безбедносни и административни зони во објектот во кој се ракува или се чуваат класифицирани информации;
- преместување или отстранување на возила без соодветна дозвола за пристап во безбедносен појас околу објектот и во административни зони во објектот во кој се ракува или се чуваат класифицирани информации;
- изработка на интерни акти за процена на безбедносниот ризик за класифицирани информации и за нивна заштита во случај на вонредни околности;
- ажурирање и корекција на евиденциите на класифицирани информации и нивно отстранување и уништување;
- обезбедување на пропишани услови за дисеминација и пренос на класифицирани информации и
- забрана за прием, ракување, отстапување и чување на класифицирани информации.
- други мерки за кои инспекторот ќе утврди дека се во функција на заштитата на класифицирани информации во субјектот на надзор.

Член 92

Постапка за едукација

Доколку при вршењето на инспекцискиот надзор инспекторот утврди неправилности од член 26, должно е да состави записник во кој ќе ја утврди сторената неправилност со укажување за нејзино отстранување во рок од осум дена и со истовремено врачување на покана за спроведување на едукација на лицето или субјектот каде што е утврдена неправилноста при вршењето на инспекцискиот надзор.

Формата и содржината на поканата за едукација, како и начинот на спроведување на едукацијата со правилник ги пропишува директорот на Дирекцијата.

Едукацијата ја организира и спроведува Дирекцијата, во рок не подолг од триесет дена од денот на приемот на решението.

Едукацијата може да се спроведе за повеќе утврдени исти или истородни неправилности за еден или за повеќе субјекти.

Доколку во закажаниот термин лицето или субјектот на кој се спроведува едукацијата не се јави на едукацијата, ќе се смета дека едукацијата е спроведена.

Доколку лицето или субјектот на кој се спроведува едукацијата се јави на закажаната едукација и истата ја заврши, ќе се смета дека е едуциран по однос на утврдената неправилност.

Доколку инспекторот при спроведувањето на контролниот надзор утврди дека се отстранети утврдените неправилности од ставот (1) на овој член, донесува заклучок со кој ја запира постапката на инспекциски надзор.

Доколку инспекторот при спроведувањето на контролниот надзор утврди дека не се отстранети утврдените неправилности од ставот (1) на овој член, поведува постапка за порамнување, односно поднесува барање за поведување на прекршочна постапка.

Доколку при вршење на повторен инспекциски надзор повторно се утврди неправилност кај истото лице, односно субјектот каде веќе еднаш е спроведена едукација за таквата неправилност, инспекторот директно поведува постапка за порамнување, односно поднесува барање за поведување на прекршочна постапка.

Дирекцијата води евиденција за спроведената едукација на начин пропишан со правилник донесен од страна на директорот на Дирекцијата.

Член 93

Ако при вршење на надзор инспекторот утврди повреда на закон и други прописи која претставува прекршок, поднесува барање за поведување на прекршочна постапка согласно одредбите од овој закон и Законот за прекршоците.

Ако при вршењето на надзорот инспекторот смета дека повредата претставува кривично дело, должен е веднаш да го извести директорот на Дирекцијата заради поведување постапка пред надлежен орган.

ГЛАВА СЕДМА

ПРЕКРШОЧНИ ОДРЕДБИ

Член 94

Глоба во износ од 3.000 до 5.000 евра во денарска противвредност ќе му се изрече за прекршок на правното лице- корисник на класифицирани информации, ако:

- не ги спроведе мерките за административна, физичка, безбедност на комуникациско – информациски системи, безбедност на лицата - корисници на класифицираните информации или индустриска безбедност на класифицираните информации, согласно со одредбите на членовите 26, 28, 29, 31, 32 и 33 на овој закон;
- при поднесување на барање за издавање на безбедносен сертификат приложи докази кои не соодветствуваат со реалните финансиски и економски услови на правното лице согласно со членот 42 на овој закон;
- не постапува со класифицираните информации, согласно со одредбата од членот 56 став 1 на овој закон (освен ако дејствието не претставува кривично дело);
- не извести за престанок на исполнетост на некој од условите врз основа на кои е издаден безбедносен сертификат, согласно со одредбите на членот 42 од овој закон.
- го попречува извршувањето на инспекцискиот надзор согласно со одредбите на членот 78 од овој закон.

Глоба во износ од 1.000 до 2.000 евра денарска противвредност ќе му се изрече за прекршок на одговорното лице во правното лице - корисник на класифицирани информации за прекршоците од став 1 на овој член.

Глоба во износ од 500 до 1.000 евра денарска противвредност ќе му се изрече за прекршок на физичкото лице - корисник на класифицирани информации за прекршоците од став 1 на овој член.

Член 95

Глоба во износ од 1.500 до 2.000 евра во денарска противвредност ќе му се изрече за прекршок на правното лице – корисник на класифицирани информации, ако не ги преземе потребните активности за прием, обработка, утврдување на корисниците и не изврши дисеминација на класифицираните информации до нив, согласно со одредбите на членот 26 на овој закон.

Глоба во износ од 1.000 до 1.500 евра денарска противвредност ќе му се изрече за прекршок на одговорното лице во правното лице - корисник на класифицирани информации за прекршокот од став 1 на овој член.

Глоба во износ од 500 до 1.000 евра денарска противвредност ќе му се изрече за прекршок на физичкото лице - корисник на класифицирани информации за прекршокот од став 1 на овој член.

Член 96

Глоба во износ од 1.500 до 2.000 евра во денарска противвредност, ќе му се изрече на правно лице кое ќе постапи спротивно на обврската од член 47 став 2 за заштита на класифицирани информации означени со степен „интерно“.

Глоба во износ од 1.000 до 1.500 евра во денарска противвредност, ќе му се изрече на одговорното лице во правното лице за прекршокот од став 1 на овој член.

Глоба во износ од 500 до 1.000 евра во денарска противвредност, ќе му се изрече на физичкото лице за прекршокот од став 1 на овој член.

Член 97

Глоба во износ од 500 до 1.000 евра во денарска противвредност, ќе му се изрече на правно лице кое спротивно на член 12 открие информација со ознака „за ограничена употреба“.

Глоба во износ од 450 до 700 евра во денарска противвредност, ќе му се изрече на одговорното лице во правното лице за прекршокот од став 1 на овој член.

Глоба во износ од 300 до 500 евра во денарска противвредност, ќе му се изрече на физичкото лице за прекршокот од став 1 на овој член.

Член 98

Глоба во износ од 500 до 1.000 евра во денарска противвредност ќе му се изрече за прекршок на офицерот за безбедност на класифицирани информации, ако:

- не исполни некоја од своите должности наведени во член 68,
- го попречува вршењето на инспекцискиот надзор согласно со одредбите на членот 78 на овој закон.

Член 99

Глоба во износ од 300 до 500 евра во денарска противвредност, ќе му се изрече на физичкото лице - создавач на класифицирана информација кој ќе постапи спротивно на член 9, став 2 и не ја направи потребната проценка за можната штета и последици.

Член 100

Глоба во износ од 150 до 300 евра во денарска противвредност, ќе му се изрече на физичкото лице - создавач на класифицирана информација кој ќе постапи спротивно на член 16 став 3 и член 18, став 2 и не го извести корисникот на класифицираната информација за промената на степенот на класификација или за нејзината декласификација.

Постапка за порамнување со издавање на прекршочен платен налог

Член 101

За прекршоците утврдени во овој закон, согласно со Законот за прекршоците, инспекторот е должен на сторителот на прекршокот да му издаде прекршочен платен налог, пред да поднесе барање за поведување на прекршочна постапка.

Инспекторот е должен да води евиденција за издадените прекршочни платни налози и за нивниот исход.

Во евиденцијата од ставот 2 на овој член се собираат, обработуваат и чуваат следните податоци: име и презиме, односно назив на сторителот на прекршокот, живеалиште, односно престојувалиште, седиште, вид на прекршокот, број на прекршочниот платен налог кој му се издава и исходот на постапката.

Личните податоци од ставот 3 на овој член се чуваат пет години од денот на внесување во евиденцијата.

Директорот со правилник ја пропишува формата и содржината на прекршочниот платен налог.

За се што не е регулирано со овој закон, во поглед на прекршочниот платен налог се применуваат одредбите од Законот за прекршоците.

Член 102

За прекршоците утврдени со овој закон, прекршочна постапка води и прекршочна санкција изрекува надлежен суд.

-

ГЛАВА 8

КАЗНЕНИ ОДРЕДБИ

Оддавање на класифицирани информации со степен „СТРОГО ДОВЕРЛИВО“ и „ДОВЕРЛИВО“

Член 103

Тој што на јавноста или на неповикано лице ќе соопшти, предаде или стори достапна информација што е класифицирана со степен „СТРОГО ДОВЕРЛИВО“ до којашто има пристап согласно закон и со тоа ќе ги загрози или повреди виталните интереси на Република Македонија, ќе се казни со затвор од 1 до 5 години.

Тој што на јавноста или на неповикано лице ќе соопшти, предаде или стори достапна информација што знае дека е класифицирана со степен „СТРОГО

ДОВЕРЛИВО“, а до која дошол на противправен начин, ќе се казни со затвор од 1 до 3 години.

Тој што на јавноста или на неповикано лице ќе соопшти, предаде или стори достапна информација што е класифицирана со степен „ДОВЕРЛИВО“ до којашто има пристап согласно закон и со тоа ќе ги загрози или повреди важните интереси на Република Македонија, ќе се казни со затвор од 1 до 3 години.

Тој што на јавноста или на неповикано лице ќе соопшти, предаде или стори достапна информација што знае дека е класифицирана со степен „ДОВЕРЛИВО“, а до која дошол на противправен начин, ќе се казни со парична казна или затвор од 6 месеци до 3 години.

Ако делото од ставовите 1 и 3 е извршено за време на воена состојба, сторителот ќе се казни со затвор од 1 до 10 години.

Обидот за делото од ставовите 2, 3 и 4 е казнив.

Ако делото од ставовите 1 и 3 е сторено од небрежност, сторителот ќе се казни со парична казна или затвор до 1 година.

Неовластено откривање на класифицирана информација употребена во судска или друга постапка

Член 104

Тој што спротивно на закон, неовластено ќе открие класифицирана информација со степен на класификација „ДРЖАВНА ТАЈНА“ за која дознал во судска или друга постапка, ќе се казни со затвор до 5 години.

Доколку класифицираната информација е со степен на класификација „СТРОГО ДОВЕРЛИВО“ или „ДОВЕРЛИВО“, сторителот ќе се казни со затвор од 1 до 3 години.

Обидот за делото од став 2 е казнив.

Ако делото од ставовите 1 и 2 е сторено од небрежност, сторителот ќе се казни со парична казна или затвор до 1 година.

ГЛАВА ОСМА

ПРЕОДНИ И ЗАВРШНИ ОДРЕДБИ

Член 105

Подзаконските акти кои произлегуваат од Законот за класифицирани информации („Службен весник на Република Македонија“ број 09/2004, 113/2007, 145/2010, 80/2012, 41/2014 и 21/2018) продолжуваат да се применуваат до денот на донесувањето на подзаконските акти утврдени со овој закон.

Подзаконските прописи предвидени со овој закон ќе се донесат во рок од шест месеци од денот на влегувањето во сила на овој закон.

Член 106

Прописите коишто регулираат прашања од областа на класифицираните информации ќе се усогласат со одредбите на овој закон во рок од една година од денот на влегувањето во сила на овој закон.

Член 107

Директорот на Дирекцијата за безбедност на класифицирани информации именуван до денот на влегувањето во сила на овој закон продолжува да ја извршува функцијата до истекот на мандатот за кој е именуван.

Член 108

Дирекцијата за безбедност на класифицирани информации од денот на влегувањето во сила на овој закон продолжува да работи како Дирекцијата за безбедност на класифицирани информации согласно со надлежностите утврдени со овој закон.

Член 109

Со денот на влегувањето во сила на овој закон, престанува да важи Законот за класифицирани информации („Службен весник на Република Македонија“ број 09/2004, 113/2007, 145/2010, 80/2012, 41/2014, 21/2018 и 83/2018).

Член 110

Овој закон влегува во сила осмиот ден од денот на објавувањето во „Службен весник на Република Македонија“.

ИЗВЕШТАЈ ЗА ПРОЦЕНКА НА ВЛИЈАНИЕТО НА РЕГУЛАТИВАТА

| | |
|--|---|
| <input type="checkbox"/> | <input type="checkbox"/> |
| <input type="checkbox"/> | <input type="checkbox"/> |
| <input type="checkbox"/> | <input type="checkbox"/> |
| <input type="checkbox"/> | <input type="checkbox"/> <input checked="" type="checkbox"/> |
| <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> | <input type="checkbox"/> <input checked="" type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> |
| <input type="checkbox"/> <input type="checkbox"/> (acquis) | <input type="checkbox"/> |
| <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> | <input type="checkbox"/> <input checked="" type="checkbox"/> |
| <input type="checkbox"/> <input type="checkbox"/> | |
| <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> | |
| <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> | |
| <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> | |

1. Опис на состојбите во областа и дефинирање на проблемот

1.1 Опис на состојбите

Со Законот за класифицирани информации се уредува системот за заштита на класифицирани информации во Република Македонија, при што се става акцент на класифицирањето на информациите, определувањето на степените на класификација, критериумите, мерките и активностите за заштита на класифицираните информации, размената на класифицираните информации со странски држави и меѓународни организации, постапките за издавање и времетраењето на безбедносните сертификати, органите за заштита на класифицирани информации, плановите и програмите за работење на Дирекцијата, вршењето надзор, прекршочните и казнените одредби при неовластено откривање на класифицирани информации, како и други прашања сврзани со системот за заштита на класифицирани информации.

Законот за класифицирани информации за прв пат беше донесен во март 2004 година, а потоа согласно потребите согледани преку неговата непосредна примена во областа која ја уредува или поради усогласување со други закони чии одредби потребно е да се имплементираат во законскиот текст, беше менуван и дополнуван шест пати („Службен весник на Република Македонија“ бр. 09/2004, 113/2007, 145/2010, 80/2012, 41/2014, 21/2018 и 83/2018). Досега не е изработен официјален пречистен текст.

Причините за донесување на овој Предлог на Закон за класифицирани информации е одржувањето на високо ниво на усогласеност со регулативите на НАТО и ЕУ, опфаќање искуства од научените лекции од примената на законот во периодот на важење на претходното законско решение и прецизирање одредени прашања од доменот на работата на надлежностите на Дирекцијата што произлегуваат од новините во одредени области и од започнатите пристапни разговори со НАТО.

1.2 Причини за проблемите кои се предмет на разгледување

Во текот на имплементацијата на Законот за класифицирани информации („Службен весник на Република Македонија“ бр. 09/2004, 113/2007, 145/2010, 80/2012, 41/2014, 21/2018 и 83/2018) утврдена е потреба за воведување законски решенија за усогласување со постојна регулатива во други области, за регулирање на прашања што претходно не биле опфатени во регулативата (како на пример, користењето на класифицираните информации во судска или друга постапка), како и за воведување законска основа за подзаконски акт којшто ја регулира криптозаштитата во земјата. Согласно интеграциските процеси на земјата во НАТО и ЕУ, согледана е и потреба за проширување на надлежностите на Дирекцијата во доменот на размената и заштитата на класифицирани информации со меѓународните организации.

2. Цели на предлог регулативата

Цел на Предлогот на Законот за класифицирани информации е уредување на системот за заштита на класифицирани информации во Република Македонија со одржување на високо ниво на усогласеност со регулативите на НАТО и ЕУ.

3. Можни решенија (опции)

3.1 *Опис на решението „не прави ништо“*

Со ова решение нема да се постигне целта заради која се предлага донесувањето на нов Закон за класифицирани информации.

Доколку не се донесе новиот текст на законот, во сила ќе останат законските решенија кои ги содржи Законот за класифицирани информации од 2004 година во којшто не се содржани одредби за усогласување со Законот за инспекциски надзор, не се регулирани надлежностите на Дирекцијата што произлегуваат од започнатите пристапни разговори со НАТО и не е дадена законска основа за донесување подзаконски акт за уредување на прашањата поврзани со криптозаштитата во Република Македонија.

3.2 *Опис на можните решенија (опции) за решавање на проблемот*

Во функција на соодветно имплементирање на прифатените меѓународни стандарди за безбедност на класифицираните информации, во Дирекцијата за безбедност на класифицирани информации беше извршена компаративна анализа на законските решенија на 12 земји членки на НАТО и на ЕУ со коишто Република Македонија има потпишано билатерална спогодба за размена и заемна заштита на класифицирани информации. Врз основа на резултатите од направената анализа и од разменетите искуства со сродните служби на земјите од регионот со коишто Дирекцијата има развиено блиска соработка, во новиот текст на законот се предложени решенија коишто одат во прилог на одржувањето на високо ниво на усогласеност на националното законодавство за класифицирани информации со регулативите на НАТО и ЕУ.

4. Проценка на влијанијата на регулативата

Можни позитивни и негативни влијанија од секоја од опциите:

4.1 *Економски влијанија*

Понудената опција нема да предизвика трошоци за економијата во областа на вработувањето и конкурентноста. Со оглед на тоа дека се нормативни решенија од процедурален карактер, нема да има влијание врз малите и средни претпријатија и други економски субјекти.

4.2 *Фискални влијанија*

Усвојувањето на предложениот закон може да наметне потреба од дополнителни финансиски средства заради потребата за изедначување на националните стандарди во контекст на примената на мерките за заштита на класифицираните информации со стандардите на НАТО и на ЕУ. Тие средства ќе бидат обезбедени од Буџетот на Република Македонија.

4.3 Социјални влијанија

Решенијата содржани во предложениот закон нема да влијаат врз намалување на сиромаштијата, заштитата и унапредувањето на здравјето, како и родовата еднаквост односно заштитата на ранливите групи и обесправените, но ќе имаат соодветни позитивни импликации врз заштитата и унапредувањето на човековите права, воопшто.

4.4 Влијанија врз животната средина

Со решенијата содржани во предложениот закон нема да се влијае врз воздухот, почвата, нема да има ефект на стаклена градина, бучава, биодиверзитет, а со тоа што нема влијание врз наведените делови на природата, нема да има ниту директно или индиректно влијание врз здравјето на луѓето.

4.5 Административни влијанија и трошоци –

а) трошоци за спроведување

Со предложениот закон е предвидена примена на соодветни мерки и активности за заштита на класифицираните информации од аспект на административната, персоналната, физичката, индустриската и информатичката безбедност коишто, заради изедначување на постојните национални стандарди за заштита на класифицираните информации со стандардите на НАТО и на ЕУ, ќе ја наметнат потребата од дополнителни финансиски средства што ќе бидат обезбедени од Буџетот на Република Македонија. Опремата и техничките средства ќе бидат пропишани во подзаконски акти.

б) трошоци за почитување на регулативата

Со предложените законски решенија не се предлага воведување на нови административни оптоварувања, формалности и трошоци, односно не се предвидени нови трошоци за издавање на лиценци, дозволи и друго за правните и физичките лица, со што не се влијае врз конкурентноста.

5. Консултации

5.1 Засегнати страни и начин на вклучување

Предлогот на новиот Закон за безбедност на класифицирани информации е резултат на работата на формираната меѓуресорска работна група во која се вклучени и надворешни стручни лица – експерти. Во работната група членуваа претставници на Министерството за одбрана, Дирекцијата за безбедност на класифицирани информации, Министерството за внатрешни работи, Министерството за надворешни работи, Агенцијата за разузнавање и Секретаријатот за европски прашања. Со решение, во работата на меѓуресорската работна група беа вклучени стручни лица од професорската фела, а во доменот на безбедноста на комуникациско-информациските системи и криптозаштитата беа извршени консултации меѓу експерти од Министерството за одбрана, Дирекцијата за безбедност на класифицирани информации, Министерството за внатрешни работи, Агенцијата за разузнавање и Центарот за управување со кризи.

За специфични прашања што се предмет на уредување во предлогот на законот, беа организирани посебни состаноци со засегнатите страни, како на пример консултации за уредување на прашањето за криптозаштита со претставници на релевантните органи на државната управа и поединечни средби со претставници на државни органи кои имаа потреба од подетално толкување на предложените законски решенија.

За прашање од надлежност на Секретаријатот за законодавство извршена е соодветна консултација по пат на пишана кореспонденција.

За дискусија по предложените законски решенија со членовите на меѓуресорската работна група за изработка на предлогот на законот беше организирана и Тркалезна маса на којашто беа поканети претставници и од судската власт, од Министерството за информатичко општество и администрација, од Управата за финансиско разузнавање, од Центарот за управување со кризи и од Народна банка на Република Македонија.

5.2 Преглед на добиените и вградените мислења

Предлогот на новиот Закон за безбедност на класифицирани информации е доставен на мислење до Секретаријатот за законодавство, Министерството за финансии, Министерството за информатичко општество и администрација, Министерството за надворешни работи, Министерството за внатрешни работи, Дирекцијата за безбедност на класифицирани информации, Агенцијата за разузнавање, Центарот за управување со кризи и Секретаријатот за европски прашања. На тркалезната маса што беше организирана за расправа по предложените законски решенија беа дадени коментари и забелешки што беа обработени и соодветно вградени во предлог-текстот на законот.

Исто така, Предлогот на закон е објавен и на ЕНЕР.

5.3 Мислењата кои не биле земен предвид и зошто

Во подоцнежна фаза од проценката на влијанието на регулативата ќе бидат земени во предвид мислењата на надлежните министерства и тела по предложената содржина.

6. Заклучоци и препорачано решение

6.1 Споредбен преглед на позитивните и негативните влијанија на можните решенија (опции)

Доколку се споредат предложени опции, Опцијата 2 – донесување на новиот Закон за класифицирани инфорамации е прифатлива опција бидејќи со предложените можни решенија се очекуваат само позитивни влијанија.

Имено, со предложените измени ќе се постигнат следните цели:

- усогласување со постојна регулатива во други области (инспекциски надзор, изречување глоби),
- регулирање на прашања што претходно не биле опфатени во регулативата (како на пример, користењето на класифицираните информации во судска или друга постапка),
- воведување правен основ за подзаконски акт којшто ја регулира криптозаштитата во Република Македонија,
- проширување на надлежностите на Дирекцијата во доменот на размената и заштитата на класифицирани информации со меѓународните организации (НАТО и ЕУ),
- одржување на високо ниво на усогласеност со регулативите на НАТО и ЕУ.

6.2 Ризици во спроведувањето и примената на секое од можните решенија (опции)

При спроведувањето и примената на предложените законски решенија, постојат ризици во однос на неможноста истите целосно да се имплементираат, да не се надминат утврдените проблеми, како и да не се исполнат потребните предуслови предвидени за практична имплементација на одредбите.

6.3 Препорачано решение со образложение

Со Предлогот на Законот за класифицирани информации се уредува системот за заштита на класифицирани информации во Република Македонија и се овозможува одржување на високо ниво на усогласеност со регулативите на НАТО и ЕУ, следење на тековните трендови во практиките при ракувањето со класифицираните информации, како и прецизирање на одредени прашања поврзани со други области што се поврзани со работата на Дирекцијата за безбедност на класифицирани информации.

Тука акцентот пред сè е на усогласувањето со Законот за инспекциски надзор, обезбедувањето заштита на лицата кои ќе пријават класифицирана

информацијата со која се прикрива пречекорување на овластување, злоупотреба на функцијата или некое друго незаконско дејствие, односно казниво дело до надлежен орган согласно Законот за заштита на укажувачите, како и пополнување на постојната правна празнина со додавање инкриминации за лицата што ќе оддадат класифицирана информација со понизок степен на класификација од „државна тајна“ (во моментот во Кривичниот законик постои инкриминација само за оддавање на државна тајна, но не и за класифицирани информации со пониските степени на класификација).

Во Предлогот на Законот за класифицирани информации се прецизираат и одредени прашања од доменот на работата на надлежностите на Дирекцијата што произлегуваат од започнатите пристапни разговори со НАТО. Имено, надлежностите на Дирекцијата се проширени во доменот на размената и заштитата на класифицирани информации со НАТО и со ЕУ преку формализирање на помошните тела за безбедност на комуникации, безбедносна акредитација, ТЕМПЕСТ авторитет, дистрибуција на критпо-клучеви и за индустриска безбедност (во насока на исполнување на барањата на НАТО).

Во предлогот на законот се дава и законска основа за донесување на Уредбата за криптозаштита, што како потреба е утврдено многу оддамна.

7. Спроведување на препорачаното решение

7.1 Потреба од менување на закони и подзаконска регулатива во областа или други сродни области

Донесувањето на Предлогот на Законот за класифицирани информации ќе предизвика потреба од менување на подзаконската регулатива во областа.

7.2 Потребни подзаконски акти и рок за нивно донесување

Донесувањето на предложениот закон имплицира донесување на нови подзаконски акти од Владата на Република Македонија во рок од шест месеци од денот на донесување на предложениот закон.

7.3 Органи на државната управа, државни органи и други органи надлежни за спроведување

За спроведување на целите на Предлогот на Законот за класифицирани информации е надлежна Дирекцијата за безбедност на класифицирани информации (член 5 од Предлогот на закон).

7.4 Активности за обезбедување на ефикасно спроведување на предлогот на закон

Надлежните органи за спроведување на законот, ќе преземаат континуирани активности со цел ефикасно спроведување на предложениот закон.

8. Следење и евалуација

8.1 Начин на следење на спроведувањето

Резултатите од предложените законски решенија ќе се следат преку континуирано следење на примената на предложениот закон.

8.2 Евалуација на ефектите од предлогот на закон и рокови

Евалуација на ефектите од предложените законски решенија може да се даде откако предложениот закон започне да се применува во праксата.

Изјава од директорот на Дирекцијата

Нацрт Извештајот за проценка на влијанието на регулативата е изготвен во согласност со Методологијата за проценка на влијанието на регулативата. Тој дава реална проценка на можните влијанија и очекуваните ефекти, како и трошоците кои се однесуваат на секоја од утврдените можни решенија (опции) за решавање на проблемот

Датум: __. __. 2018 година

.....
потпис на директорот

Изјава од министерот

Врз основа на резултатите од анализите прикажани во Извештајот за проценка на влијанието на регулативата сметам дека препорачаното решение (опција) претставува најдобар начин за решавање на проблемот и постигнување на очекуваните ефекти на најекономичен начин.

Датум: _____

.....

ПОТПИС НА МИНИСТЕРОТ