РЕПУБЛИКА СЕВЕРНА МАКЕДОНИЈА
REPUBLIKA E MAQEDONISË SË VERIUT

ДКСК KSHPK
ДРЖАВНА КОМИСИЈА ЗА СПРЕЧУВАЊЕ НА КОРУПЦИЈАТА
KOMISIONI SHTETËROR PËR PARANDALIMIN E KORRUPSIONIT

Бр. 11-1289/2
10-06-2025 20___
Скопје

ДО
МИНИСТЕРСТВО ЗА ДИГИТАЛНА ТРАНСФОРМАЦИЈА
Ул.„Филип Втори Македонски„ бр.11
1000 Скопје

ПРЕДМЕТ: Мислење по предлог на Закон за безбедност на мрежни и информациски системи

Врска : Ваш бр.10-730/2 од 02.04.2025 година

Почитувани,

До Државната комисија за спречување на корупцијата на ден 14.04.2025 година од страна на Министерството за дигитална трансформација доставено е Барање на мислење на Предлог на Закон за безбедност на мрежни и информациски системи бр.10-730/2 од 02.04.2025 година.

По разгледување на доставениот предлог-текст од аспект на одредбите од Законот за спречување на корупцијата и судирот на интереси ("Службен весник на Република Македонија" бр.12/19) Државната комисија, го дава следното

М И С Л Е Њ Е

Со предлог законот се уредуваат секторите на кои се однесува законот, се утврдуваат надлежните органи за управување со сајбер кризи, единствената точка за контакт за сајбер безбедност и тимовите за одговор на инциденти со компјутерска безбедност, се уредуваат мерките за безбедност на мрежни и информациски системи и за управување со ризикот за сајбер безбедност, обврските за известување за сите аспекти на безбедност на мрежни и информациски системи за правните лица кои обезбедуваат услуги во критични сектори, правилата и обврските за известување и размена на информации за инциденти, обврската за усвојување на стратешкиот документ кој ја опфаќа безбедноста на мрежните и информациските системи, надзорот над спроведувањето на одредбите од законот, како и други прашања поврзани со безбедност на мрежни и информациски системи.

Цели на предметниот предлог закон се изградба на капацитети за безбедност на мрежни и информациски системи во државата, намалување на заканите за мрежните и информациските системи што се користат за обезбедување основни услуги во клучните сектори и обезбедување на континуитет на таквите услуги во случај на инциденти, со што се придонесува кон

безбедноста на Република Северна Македонија и ефективно функционирање на нејзината економија и општество.

Согласно образложението на предлагачот, со предлог законот се врши транспозиција на Директивата 2022/2555 на Европскиот парламент и Советот од 14 декември 2022 година за мерките за високо заедничко ниво на сајбер - безбедноста низ Унијата, за изменување на Регулативата 910/2014 и Директивата 2018/1972 и за укинување на Директивата 2016/1148.

Основаноста и потребата за донесување на предлог законот за Државната комисија не е предмет на анализа, имајќи го во предвид значењето на областа која ја регулира истиот, но од аспект на одредбите од Законот за спречување на корупцијата и судирот на интереси („Службен весник на Република Македонија" бр.12/19), применувајќи ја Методологијата за антикорупциска проверка на легислативата, се наиде на постоење на регулаторни ризици, за кои се препорачува да бидат надминати со цел подобрување на предложениот законски текст.

1. Имено, од номотехнички и редакциски аспект потребно е да се доуреди содржината на предлог законот, а особено во делот на нумерирање на ставови, точки и алинеи, како што впрочем е случај со одредбите на **член 12** во кој се утврдени надлежностите на надлежниот орган за безбедност на мрежни и информациски системи.

2. Во **член 3 точка 35)** со понаслов **Дефиниции** во смисла на овој закон **„офицер за сајбер безбедност"** е лице кое задолжително се ангажира кај суштинските субјекти кое има *соодветни посебни работни компетенции* и кое е одговорно за спроведување на мерките за сајбер безбедност утврдени со овој закон и кое е во директна комуникација и соработува со надлежниот орган и надлежниот тим за одговор на компјутерски инциденти за доследна имплементација на одредбите од овој закон.
Во вака формулираната одредба Државната комисија смета дека не е јасно дефинирано што може да се подразбере под зборовите *„соодветни посебни работни компетенции„*. Имајќи предвид дека оваа област за прв пат се уредува со закон и овие прашања не се уредени со друг материјален закон, се оцени за потребно во поимниците на предложениот закон да биде јасно пропишано што се подразбира под поимот *„соодветни посебни работни компетенции„* како услов за ангажирање на офицер за сајбер безбедност, дотолку повеќе што предлагачот на законот во членот 25 го пропишал потребното образование кое треба да го има тоа лице, но не и потребни посебни работните компетенции.
Со цел онезвозможување на субјективно толкување и различна примена на наведената одредба, се препорачува да се доуреди точката 35) од членот 3 на Предлог на Законот при што јасно да се дефинира што се подразбира под изразот „соодветни посебни работни компетенции".

3. **Во член 25 став (3)** е пропишано дека „офицерот за сајбер безбедност од ставот (1) на овој член се назначува од редот на вработените со завршено високо образование од областа на ИКТ, телекомуникациите, безбедност или право врз основа на неговите стручни квалификации, а особено врз основа на стручни знаења за сајбер безбедноста".
Во конкретниот случај, образованието „право" не е сродно со претходно утврденото образование од областа на ИКТ, телекомуникации или безбедност. Притоа, не е јасно дали лице со завршено високо образование од областа „право" ќе биде компетентно и ќе поседува знаење и стручност да биде назначено за офицер за сајбер безбедност, имајќи ја предвид специфичната област која се уредува со овој закон. Дотолку повеќе не е јасно ниту дали лице со завршено образование

безбедност ќе биде целосно компетентно и ќе поседува знаење и стручност за исполнување на овластувањата пропишани за офицерот за сајбер безбедност. Ова произлегува од комплексноста на задачите и овластувањата кои ги пропишува предложениот текст на законот во ставот (4) од истиот член, како што се: спроведување и/или надзор на соодветната примена на одредбите содржани во овој закон, други подзаконски акти и интерни акти; изработка и спроведување на сајбер безбедносна програма која ќе опфати политики, процедури и мерки за заштита од сајбер напади и зголемување на сајбер отпорноста на информациски технологии и оперативни технологии; откривање на структурни и системски слабости и ризици во информациско комуникациските системи и мрежи, како и во физичката и виртуелната инфраструктура; дефинирање на сценарија и процена на ризици по сајбер безбедноста во процесот на воспоставување на систем за управување со ризици; редовно следење на ранливоста на системите, следење и процена на актуелните опасности кон мрежните податоци и воведување мерки за ублажување на последиците од сајбер инциденти; обезбедување на ажурирање на хардверските уреди и софтверските апликации.
Дополнително регулаторен ризик постои и доколку се земе предвид дека институциите имаат должност „да назначат" **еден или повеќе** административни службеници како офицери за сајбер безбедност, па во случај едно лице да биде овластено како офицер за сајбер безбедност, оправдано се јавува сомневањето дали лице со завршено високо образование „право" или „безбедност" како единствено лице за сајбер безбедност ќе биде во можност соодветно, квалитетно и ефикасно да одговори на вака дадените задачи и овластувања утврдени со законот, односно дали овластување на лице со завршено образование од областа на правото како офицер за сајбер безбедност, претставува гарантен механизам за преземање на законски пропишани мерки за безбедност на мрежните и информациските системи во институциите.
Согласно наведеното Државната комисија препорачува да се преиспита дали лице со завршено високо образование од областа на правото или од областа на безбедноста може да биде назначено како лице за офицер за сајбер безбедност.

4. Регулаторен ризик Државата комисија утврди и во **став (11) од членот 25** со кој е пропишано дека: „Поблиските стручни квалификации, општи и посебни компетенции за офицер за сајбер безбедност во институциите од член 4 став (1) од овој закон ги пропишува министерот".
Со вака пропишаната одредба од став (11) на овој член останува нејасно кои стручни квалификации треба да ги поседува лицето, како и стручни знаења и практики, без притоа да се наведат на пример потребни години на работно искуство во струката, работа во одредена област или други стручни квалификации.
Иако во став (3) од наведениот член предлагачот има пропишано дека ова лице ќе се назначува од редот на вработените врз основа на неговите стручни квалификации, а особено врз основа на стручни знаења за сајбер безбедноста и практиките во областа на сајбер безбедноста, евидентно е дека во став (11) не ги утврдил критериумите, туку само пропишал дека поблиските стручни квалификации и посебни компетенции ќе ги пропише министерот. За да бидат уредени поблиску овие стручни квалификации, најпрвин треба да бидат пропишани со закон, по што може понатаму да се доуредуваат со подзаконски акт.
Во спротивно, вака пропишаната одредба од став (11) на овој член остава простор да се искористи дискреционото право на министерот при уредување на овие услови што треба да ги поседува офицерот за сајбер безбедност во институциите.
Со цел да се ограничи дискреционото право на министерот и да се минимизира регулаторниот ризик, Државната комисија препорачува во предложениот законски текст да се утврдат стручните квалификации, условите и критериумите, кои понатаму може поблиску да се доуредат

со донесување на подзаконски акт. Дополнително, согласно позитивното право на Република Северна Македонија само со закон се пропишуваат права, обврски, услови и критериуми, додека со подзаконски акт може да се даде поблиско објаснување и дефинирање на условите, да се определи начинот, формата, содржината и постапката.

Наведените забелешки и препораки се однесуваат и на **член 42 став (1) и став (5)** со кој се утврдува потребното образование и уредувањето на посебни стручни квалификации, општи и посебни компетенции на овластеното лице за вршење на стручен надзор над спроведување на законот.

5. **Во член 26** со поднаслов **Национален координатор за безбедност на мрежни и информациски системи** е пропишано дека:

„Член 26

(1) Владата на предлог на министерот назначува Национален координатор за безбедност на мрежни и информациски системи.
(2) Националниот координатор за безбедност на мрежи и информациски системи го координира разменувањето на податоци и информации поврзани со безбедност на мрежните и информациските системи во и надвор од државата.
(3) Националниот координатор за безбедност на мрежи и информациски системи го координира настапот на надлежните органи во меѓународните организации".

Недостигот на критериуми за избор, недефинирани услови и фази во постапката за назначување на Националниот координатор за безбедност на мрежни и информациски системи, создава правна празнина и недефиниран опсег на законот. Имајќи ги во предвид овластувањата што предложениот закон му ги дава на назначеното лице, на национално како и на меѓународно ниво, вака пропишаната одредба создава ризик да не биде назначено лице со интегритет, стручност и потребни квалификации од оваа област, туку остава простор за дискреционо одлучување и ризик за влијание на оние кои го назначуваат.
Согласно наведеното, Државната комисија препорачува да се допрецизира одредбата со јасно пропишани услови, критериуми и постапка за назначување на Националниот координатор за безбедност на мрежи и информациски системи.

6. Во **член 36** од Предлог на Законот е пропишано дека:

„Член 36

(1) Министерството утврдува стандарди за безбедност на мрежните и информациските системи усогласени со ЕУ и меѓународните стандарди, како и упатства за нивна имплементација.
(2) Министерството во соработка со Бирото за јавни набавки изготвува модели на технички спецификации за набавка на мрежни и информациски системи кои ќе бидат усогласени со меѓународните стандарди.
(3) Врз основа на упатставата од став (1) на овој член Министерството воспоставува и води Регистар на ИКТ – услуги, ИКТ – системи и ИКТ- производи и нивни производители со висок ризик, кои нема да се земаат во предвид, односно се исклучуваат при постапките за јавни набавки."

Законодавецот во став (3) од овој член пропишал обврска за Министерството да воспоставува и да води Регистар, но притоа останува нејасно што се подразбира под изразот „производители со висок ризик„ кој за прв пат се споменува во предложениот законски текст. Воедно, во членот 3 од предложениот закон каде се дефинирани изразите ИКТ производ, ИКТ услуга, предлагачот на законот пропуштил да го дефинира изразот „производители со висок ризик" поради што се остава простор од двосмислено толкување при примена на одредбата и можна злоупотреба на дискреционото одлучување. Оттука се јавува потребата сите користени термини и изрази во предложениот текст на законот да бидат јасно пропишани и дефинирани.
Имајќи ги во предвид последиците кои произлегуваат од ставот (3) на членот 36, а со цел да не се остави можност на субјективно толкување и различна примена, Државната комисија препорачува изразот „производители со висок ризик„ да се дефинира во поимникот на предложениот закон во членот 3, со јасни објективни критериуми.

7. Со **членот 40** се уредува правото на додаток на плата на таксативно утврдени категории на вработени во институциите од член 4 став (1) на овој закон, заради специфичност на работните задачи и прилагодување на пазарот на труд. Согласно точка 4) од ставот (1) на член 40, право на наведениот додаток на плата во износ од 50% од основната плата имаат и офицерите за сајбер безбедност од член 25 став (1) на предложениот закон. Воедно, со став (2) на членот 40 е утврдено дека работните места во организациската единица за сајбер безбедност во надлежниот орган од член 12 став (1) од овој закон, како и работните места за лицата од ставот (1) точки 2), 3) и 4) (на овој член) во институции од јавен сектор може да бидат пополнети со лица со завршено високо образование од областа на ИКТ, телекомуникации, безбедност или право, кои ги исполнуваат општите и посебните услови утврдени со актот за систематизација.
Од анализата на вака наведените одредби на член 40 став (1) точка 4) и став (2), како и одредбите од член 3 точка 35), член 8 став (6) и член 25 став (1) на овој закон, се утврди постоење на т.н. внатрешен конфликт на истите, што претставува регулаторен ризик од корупција.

Имено, со член 3 точка 35) предлагачот го дефинирал офицерот за сајбер безбедност како „лице кое задолжително се ангажира", а со ставот (6) на член 8 како „лице кое задолжително се овластува".

Додека пак, со членот 25 став (1) институциите од член 4 став (1) од овој закон во зависност од видот и бројот на мрежни и информациски системи и бројот на вработени во институцијата се должни „да назначат" еден или повеќе административни службеници како офицери за сајбер безбедност. Притоа, назначувањето на административен службеник распореден на определено работно место во институцијата кое не е поврзано со задачите и овластувањата утврдени во став (4) на членот 25, како офицер за сајбер безбедност, подразбира дополнителна работна задача за тоа лице.

Истовремено, од одредбата на ставот (2) на член 40 недвосмислено произлегува дека за офицер за сајбер безбедност треба да биде предвидено работно место во актот за систематизација и утврдува кое образование е соодветно за негово пополнување, односно предвидено е идентично образование согласно образованието утврдено во член 25 став (3) од предложениот закон.

Вака наведените одредби во однос на статусот на офицерот за сајбер безбедност во институциите, се двосмислени, нејасни, контрадикторни и може да бидат предмет на субјективно толкување и различна примена од институциите.

Дополнително, Државната комисија ги зеде во предвид одредбите од **член 39** со кои се уредува правото и должноста на специјализирани обуки на вработените во тимовите за одговор на компјутерски инциденти, вработените во организациските единици за сајбер безбедност и офицерите за сајбер безбедност, како и обврските кои согласно став (5) на овој член се уредуваат со писмен договор во кој помеѓу останатото се утврдува и точниот датум до кој вработениот не може да побара престанок на работниот однос како и неговата материјална одговорност во случај на престанок на работниот однос по негова вина или на негово барање пред утврдениот датум. По анализа на истите, недвосмислено може да се заклучи дека предлагачот на законот офицерот за сајбер безбедност го третира како вработен на работно место офицер за сајбер безбедност или вработен во организациска единица за сајбер безбедност, а не како назначено лице од редот на вработените во институциите на работни места во чиј делокруг не се опфатени работни задачи за сајбер безбедност, мрежни и информациски системи итн.

Оттука, Државната комисија цени дека е потребно предлагачот на законот да го ревидира статусот на офицерот за сајбер безбедност утврден во член 25 став (1) и став (3) од предложениот закон и истиот таксативно да го утврди како работно место во актот за систематизација на работни места во институциите кои имаат обврска да имаат таков офицер, како што впрочем упатува и членот 40 став (2) од предложениот закон. Воедно, по ревидирање на статусот на офицерот за сајбер безбедност, потребно е и негово усогласување со дефиницијата за офицер за сајбер безбедност пропишана во член 3 точка 35) од предложениот закон, а особено во делот „задолжително се ангажира“, како и во ставот (6) на членот 8 во делот „задолжително овластуваат“, со цел да се избегне ризикот од субјективно толкување и различна примена на одредбите од законот кои се однесуваат на наведеното лице но, и запазување на правата и обврските кои произлегуваат за него.

8. По анализа на целокупниот предложен текст на законот, се оцени за потребно од негово редакциско подобрување, како и користење на воедначена терминологија, а особено кога се упатува на надлежност на определено лице, како што е случајот со истовремено користење на изразот „министер“ и изразот „министер за дигитална трансформација“ во ставот (9) на членот 39.

Дополнително, Државната комисија препорачува во предложениот текст на законот, онаму каде е возможно и спроведливо, да се утврдат прецизни рокови, особено во одредбите кои предвидуваат обврски за донесување годишни планови и други документи поврзани со спроведување на обврските кои произлегуваат од ваквото законско решение.

При спроведување на антикорупциската проверка и дефинирање на дадените препораки, Државната комисија ја зема во предвид целта на предложениот закон во смисла на обезбедување на високо ниво на безбедност и заштита на мрежни и информациски системи.

Од аспект на примена на Методологијата за антикорупциска проверка на легислативата, а со цел да се минимизираат утврдените регулаторни ризици, Државната комисија го доставува предметното мислење.

Воедно се укажува на потребата навремено да известите за преземените активности во насока на надминување на утврдените регулаторни ризици, односно образложение за препораките кои не се прифатени.

Заменик претседател,

м-р Билјана Каракашова Шулев

Изработил: С.И.,советник
Проверил:А.С., раководител на одделение
Контролирал:Б.В.Б., помошник раководител на сектор
Одобрил:М.К., раководител на сектор