**ИЗВЕШТАЈ ЗА ПРОЦЕНКА НА ВЛИЈАНИЕТО НА РЕГУЛАТИВАТА**

|  |  |
| --- | --- |
| Назив на министерство: | Министерство за дигитална трансформација |
| Назив на предлогот на закон: | Закон за безбедност на мрежни и информациски системи |
| Одговорно лице и контакт информации: |  |
| Вид на Извештај | Нацрт  Предлог |
| Обврската за подготовка на предлогот на закон произлегува од: | Годишната програма за работа на Владата на Република Северна Македонија  НПАА  Заклучок на Владата на Република Северна Македонија  Друго\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| Поврзаност со Директивите на ЕУ | ДИРЕКТИВА (ЕУ) 2022/2555 НА ЕВРОПСКИОТ ПАРЛАМЕНТ И НА СОВЕТОТ од 14 декември 2022 година за мерките за високо заедничко ниво на кибербезбедност низ Унијата, за изменување на Регулативата (ЕУ) бр. 910/2014 и Директивата (ЕУ) 2018/1972 и за укинување на Директивата (ЕУ) 2016/1148 (Директива NIS 2) |
| Дали нацрт извештајот содржи информации согласно прописите кои се однесуваат на класифицираните информации | Да  Не |
| Датум на објавување на нацрт Извештајот на ЕНЕР: | 18.12.2024 |
| Датум на доставување на нацрт Извештајот до Министерството за јавна администрација: |  |
| Датум на добивање на мислењето од Министерството за јавна администрација: |  |
| Рок за доставување на предлогот на закон до Генералниот секретаријат |  |

**1. Опис на состојбите во областа и дефинирање на проблемот**

***1.1 Опис на состојбите***

Мрежните и информациските системи претставуваат основа за современото функционирање на дигиталната економија и општеството во целина. Во Република Македонија, значителен дел од јавните процеси се базираат на информациските и комуникациските технологии (ИКТ), што ги прави значајни за националната безбедност и економската стабилност.

Отсуството на сеопфатна правна регулатива за безбедноста на мрежите и информациските системи доведе до недоволна заштита од сајбер закани, напади и неовластен пристап. Во тој контекст, потребно е воспоставување на законска рамка која ќе ги уреди односите меѓу сите релевантни чинители, вклучително и приватниот сектор, со цел зајакнување на сајбер безбедноста на национално ниво.

Дополнително, Република Северна Македонија, како земја во процес на пристапување кон Европската унија, има обврска да ја транспонира Директивата (ЕУ) 2022/2555 (НИС2), која поставува стандарди за високо ниво на заштита на мрежите и информациските системи низ Унијата. Транспонирањето на оваа директива ќе овозможи унапредување на националната сајбер безбедност.

Со новиот закон ќе се уредат мерките за управување со ризиците, процедурите за известување за сајбер инциденти, и ќе се утврдат надлежните органи за надзор и координација. Овој пропис е клучен за обезбедување на сигурна и доверлива дигитална околина во која граѓаните и бизнисите ќе можат да функционираат безбедно.

**2. Цели на предлог регулативата**

Целите на овој закон се идентификација на секторите од клучно значење за мрежната и информациската безбедност, обезбедување ефикасна заштита и воспоставување високо ниво на сајбер безбедност, со крајна цел заштита, одржлив развој и понатамошен напредок на општеството. Преку транспонирање на Директивата (ЕУ) 2022/2555 (НИС2) во националното законодавство се зајакнува националната отпорност кон сајбер закани. Дополнително, со овој закон се има за цел подобрување на координацијата помеѓу јавните институции, приватниот сектор и меѓународната соработка. Исто така, законот ќе придонесе за јакнење на човечките и техничките капацитети преку соодветни обуки и воспоставување институционална рамка која вклучува надлежни органи за сајбер безбедност, национална стратегија за сајбер безбедност и единствена точка за контакт.

**3. Можни решенија (опции)**

**Проценка на влијанијата на регулативата**

***Можни позитивни и негативни влијанија од секоја од опциите:***

***4.1 Економски влијанија***

Понудената опција ќе предизвика трошоци во областа на платите на вработените и конкурентноста, но нема да има влијание врз малите и средни претпријатија.

***4.2 Фискални влијанија***

За усвојување на предложениот закон се потребни дополнителни фискални средства.

***4.3 Социјални влијанија***

Предлог законот за безбедност на мрежните и информациските системи ќе има значајни социјални влијанија, вклучувајќи подобрување на довербата на граѓаните во дигиталните услуги, намалување на ризикот од сајбер криминал, создавање нови работни места, поттикнување на дигиталната инклузија и јакнење на свеста за сајбер безбедност. Исто така, законот ќе придонесе за унапредување на човековите права преку обезбедување мерки за заштита на личните податоци, кои би можеле да се разменуваат преку информациско-комуникациските технологии, како и за поддршка на едукативни и истражувачки иницијативи и намалување на дигиталниот јаз. Дополнително, имплементацијата на законот ќе ја зголеми довербата во јавните институции и ќе придонесе за создавање сигурно и доверливо дигитално општество.

***4.4 Влијанија врз животната средина***

Со предложените решенија нема да се влијае врз воздухот, почвата, нема да има ефект на стаклена градина, бучава, био-диверзитет, 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**

Имплементацијата на законот ќе предизвика административни влијанија и трошоци, вклучувајќи потреба од нови човечки ресурси, нивна обука и можни инвестиции во канцелариски простор. Дополнително, ќе бидат неопходни трошоци за опремување, како што се набавка на современа опрема, софтверски решенија и безбедносни алатки, кои ќе обезбедат ефикасно спроведување на законските обврски и унапредување на сајбер безбедноста

***б) трошоци за почитување на регулативата***

Со предложените законски решенија не се очекува 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***

* Меѓу секторска работна група за подготовка на Предлог законот за безбедност на мрежни и информациски системи;
* јавна објава на текстот на законот на ЕНЕР и
* организирање на неколку јавни расправи

***Преглед на добиените и вградените мислења***

***5.3 Мислењата кои не биле земени предвид и зошто***

**6. Заклучоци и препорачано решение**

***6.1 Споредбен преглед на позитивните и негативните влијанија на***

***можните решенија (опции)***

Целта на овој закон е обезбедување високо заедничко ниво на безбедност и заштита на мрежни и информациски системи заради непрекинато функционирање на внатрешниот пазар, превенција на сајбер безбедносни инциденти или кризи, како и развој на брза и ефективна оперативна соработка за заштита на мрежи и информациски системи.

* 1. ***Ризици во спроведувањето и примената на секое од можните***

***решенија (опции****)*

При спроведувањето и примената на предложените законски решенија не постојат ризици.

***6.3 Препорачано решение со образложение***

Усвојување на предлог законот за безбедност на мрежни и информациски системи.

**7. Спроведување на препорачаното решение**

***7.1 Потреба од менување на закони и подзаконска регулатива во***

***областа или други сродни области***

Со донесување на предметниот закон, а со цел обезбедување унифицираност и конзистентност во правниот систем на Република Северна Македонија, можни се измени во Законот за електронските комуникации.

***7.2 Потребни подзаконски акти и рок за нивно донесување***

Дополнително ќе бидат утврдени

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

Одредбите на овој закон се применуваат на работата на Владата на Република Северна Македонија, органите на државната управа, другите органите на централната државна власт, општините, општините во Градот Скопје и Градот Скопје.

***7.4 Активности за обезбедување на ефикасно спроведување на предлогот на закон***

Министерството за дигитална трансформација ќе преземе активности за целосна имплементација на предметните решенија.

**8. Следење и евалуација**

* 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***

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