Почитувани,

По сериозно разгледување на текстот на Предлог Законот за безбедност на мрежи и информациски системи („**Предлог Закон**“), во прилог ви ги доставуваме нашите предлози, коментари и измени.

Со почит,

Адвокат Љупка Новеска Андонова

**КОМЕНТАРИ, ПРЕДЛОЗИ И ИЗМЕНИ НА ПРЕДЛОГ ЗАКОН ЗА БЕЗБЕДНОСТ НА МРЕЖИ И ИНФОРМАЦИСКИ СИСТЕМИ**

|  |  |
| --- | --- |
| **Член од Предлог Законот** | **Коментар** |
| **Член 4 став 1**(1) Овој закон задолжително се применува на Владата на Република Северна Македонија, органите на државната управа, другите органите на централната државна власт, општините, општините во Градот Скопје и Градот Скопје. | Сметаме дека општините, општините во Градот Скопје и Градот Скопје треба да бидат исклучени од примената на Предлог Законот од следниве причини:1. Различни размери на ризик: Владата и централните државни органи обично управуваат со критична национална инфраструктура, бидејќи таа има пошироки импликации за националната безбедност. Општините генерално работат на помали, локализирани размери, така што нивото на системски ризик не е исто. Ова е особено точно бидејќи општините обично се занимаваат со локализирани административни функции и податоци, кои можеби нема да привлечат исто ниво на киберзакани како системите на централната власт. Дополнително, општините ретко работат со критични системи.
2. Ограничени ресурси: Општините и општините во Градот Скопје често работат со ограничени финансиски и технички ресурси. Наметнувањето обврски за усогласеност со сложените прописи за кибербезбедност, особено ако се земе предвид аргументот под точка 1 погоре, може да претставува значителен товар. Дополнително, спроведувањето на мерките за кибербезбедност може да бара одредено ниво на стручност на вработените, што општините го немаат. Ова може да предизвика натамошни неефикасности во работењето на општините и општините во Градот Скопје, вклучително и непотребно административно оптоварување.
3. Дуплирање на напорите: Доколку Предлог Законот предвидува механизми за централизиран надзор и координација на државната управа и владините органи, во областа на кибербезбедноста, барањето општините да донесат посебни мерки може да резултира со преклопување на надлежностите и неефикасност. Наместо тоа, централната власт може индиректно да ја прошири заштитата на општините, преку обезбедување на пошироката мрежна инфраструктура.

Како алтернатива на горенаведеното, на општините, општините во Градот Скопје и Градот Скопје треба да им се обезбедат насоки или најдобри практики за подобрување на кибербезбедноста, наместо да се наметнува задолжително усогласување. |
| **Член 15, став 6**Министерството соработува со надлежното регулаторно тело за електронски комуникации во Република Северна Македонија за координирани проценки на безбедносни ризици кај добавувачи и производители на мрежна опрема за операторите, а исто така соработува и со други домашни надлежни институции и тела за координирани проценки на безбедносни ризици на суштински ланци на снабдување на ИКТ-услуги, ИКТ-системи и ИКТ-производи, земајќи ги предвид техничките и не-техничките фактори на ризик. Притоа Министерството ги има предвид идентификуваните фактори на ризик од страна на институциите на Европската Унија.  | Се оваа одредба се дозволува вклучување на не-технички фактори во проценките на ризикот, што, како импликација, може да вклучи геополитички околности, земјата на потекло на производителот, економската стабилност на земјата и други субјективни критериуми. Сепак, овие фактори честопати е тешко објективно да се измерат и може да доведат до предрасуди што директно не ги одразуваат способностите за кибербезбедност или безбедносната положба на производителот.Конкретно, оваа одредба споменува координирани проценки на ризикот спроведени од надлежните органи, врз основа на техничките и не-техничките фактори, притоа земајќи ги предвид факторите на ризик идентификувани од институциите на Европската унија (ЕУ). Вклучувањето на не-технички фактори предизвикува загриженост бидејќи може да влијае врз објективноста и да доведе до неколку потенцијални проблематични прашања. Проценките на ризикот за кибербезбедноста треба да се засноваат на јасни, објективни и технички критериуми, потпирајќи се на добро воспоставени и признати стандарди.Одредбата е доста широка во однос на давање значителна дискреција на надлежните органи да утврдат како техничките и не-техничките фактори на ризик се мерат и се применуваат во проценките. Од ова произлегуваат неколку потенцијални прашања, како што се недостаток на транспарентност, ризик од фаворизирање и дискриминација, непредвидлива деловна средина, потенцијално наштетување на пазарната конкуренција итн.Принципот на неутралност во однос на технологии е од клучно значење за да се осигура дека законот нема неправедно да фаворизира одредени технологии, добавувачи или производители. Неутралноста во однос на технологиите бара безбедносните прописи да се применуваат подеднакво за сите производители, без оглед на нивното потекло, технолошкиот стек (technology stack) или деловни практики, се додека тие ги исполнуваат неопходните стандарди за кибербезбедност. Сепак, вклучувањето на не-технички фактори на ризик од предложената одредба може неправедно да им нанесе неповолна положба на одредени производители, особено оние надвор од ЕУ, дури и кога нивната технологија е во согласност со воспоставените технички стандарди и стандарди за кибербезбедност.Исто така, дозволувањето да се земат предвид овие не-технички фактори може да ги исклучи странските добавувачи и производители кои инаку би можеле да донесат ефективни, иновативни и технолошки напредни решенија. За Република Северна Македонија, потпирањето на ограничен фонд на производители поради субјективни, не-технички фактори може да доведе до повисоки трошоци и производи со понизок квалитет за потрошувачите и бизнисите. Исто така, се ризикува да се намали пазарната конкуренција, што може да и наштети и на локалната економија и на технолошкиот екосистем на долг рок. Ваквиот ризик за пазарната конкуренција не е во согласност со Законот за заштита на конкуренцијата („Службен весник на Република Македонија“ бр. 145/2010, со сите измени и дополнувања), чија цел е „*да се обезбеди слободна конкуренција на домашниот пазар со цел да се поттикне економската ефикасност и благосостојбата на потрошувачите*.“Понатаму, на новите односно малите производители, особено оние надвор од ЕУ, им се отежнува исполнувањето на вака широки и често субјективни безбедносни критериуми кои ги надминуваат обичните технички критериуми. Ова ненамерно може да создаде бариери за влез на помалите компании кои се исто толку способни, но се обесправени од пошироките, не-технички критериуми за оценување.Одредбата се однесува и на разгледување на факторите на ризик, идентификувани од институциите на ЕУ. Иако усогласувањето со стандардите и рамките на ЕУ може да обезбеди значителни придобивки во однос на хармонизацијата и соработката во кибербезбедноста, постои загриженост дека фокусот на ризичните фактори на ЕУ од страна на Предлог Законот може да воведе пристрасност во корист на производителите или технологиите кои потекнуваат од ЕУ. Ова може да значи потенцијално ставање во неповолна положба за производителите кои не се членки на ЕУ, особено оние во земји со многу различни регулаторни средини за кибербезбедност. Предлог Законот, со упатување на не-технички фактори на ризик, може ненамерно да ги фаворизира компаниите или технологиите на ЕУ, иако компаниите кои потекнуваат од држави кои не се членки на ЕУ може да понудат еквивалентни, ако не и супериорни решенија за кибербезбедност.Термините употребени во одредбата, како што се „*не-технички фактори*“, „*проценки на безбедносни ризици*“ и „*координирани проценки*“, се широки и недефинирани, што остава простор за широка дискреција во толкувањето. Оваа нејаснотија создава правна несигурност за субјектите и производителите кои сакаат да ги разберат нивните обврски согласно законот. Затоа, од суштинско значење е дефинирање на објективни критериуми за проценка на ризикот, при што не-техничките фактори не треба да се земат во предвид.**Препораки:**За да се одговори на овие проблеми, во одредбата би можело:* да се избришат не-техничките фактори за да се спречи нејасно и дискреционо одлучување;
* да се воспостават транспарентни и добро дефинирани критериуми за проценка на ризикот, фокусирајќи се првенствено на објективни технички фактори како што се безбедносни стандарди, сертификати и мерки за перформанси;
* да се даде приоритет на неутралност во однос на технологиите, осигурувајќи дека ниту еден производител или технологија не е неправедно исклучен или фаворизиран врз основа на субјективни, не-технички околности.

Овој пристап ќе создаде попредвидлив, праведен и конкурентен пазар на решенија за кибербезбедност, од корист и за потрошувачите и за бизнисите во Република Северна Македонија. |
| **Член 34****Стандардизација**(1) Со цел промовирање на конвергентна имплементација на членот 30 ставови (1), (2) и (3) од овој закон, без наметнување или дискриминација во корист на употреба на одредена технологија, Министерството поттикнува користење европскии меѓународни стандарди и технички спецификации за безбедност на мрежни и информациски системи.(2) Министерството во транспарентна постапка изготвува упатства во однос на техничките области од ставот (1) на овој член, како и во однос на веќе постојните меѓународни и национални стандарди. (3) Врз основа на упатствата од ставот (2) 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.  | Оваа одредба, која се однесува на стандардизација на мерките за управување со ризик од кибербезбедноста, резултира со неколку големи пропусти, вклучувајќи нејасни критериуми, прашања за транспарентност, потенцијал за дискриминација, ризик од злоупотреба, несигурност во спроведувањето на одредбата, итн.Терминот „*производители со висок ризик*“ е воведен без никакви придружни дефиниции или специфични фактори на ризик кои би предизвикале таква класификација. Оваа одредба не обезбедува никаква детална методологија за тоа како се проценува ризикот или кои специфични критериуми би го категоризирале производителот како високоризичен. Без јасни објективни критериуми, одлуката се сведува на дискрецијата на Министерството или релевантните органи, што може да доведе до субјективно толкување и дискриминаторски практики.Понатаму, неизвесноста за тоа како се составува списокот на производители со висок ризик и кој ќе биде засегнат од овие одлуки, резултира со одредба во која недостига транспарентност и одговорност. Имено, оваа одредба го одредува создавањето на Регистар на ИКТ-услуги, ИКТ-системи и ИКТ-производи и нивни производители со висок ризик („**Регистар**“), но не содржи детали во однос на критериумите за инклузија, кој ќе одлучува за таквите критериуми, колку често ќе се ажурира Регистарот, како производителите ќе бидат информирани за нивниот статус или каков ќе биде процесот на жалба (ако е воопшто предвиден). Широката дискреција што им се дава на органите за дефинирање и управување со Регистарот, како и нејасната практична примена на оваа одредба, може да доведе до злоупотреба од страна на Министерството или надлежните органи. Покрај тоа, иако одредбата му дава овластување на Министерството да управува со Регистарот, истата не содржи јасни регулаторни заштитни мерки за да се спречи злоупотреба, како што се воспоставени кочници и рамнотежи во процесот на донесување одлуки за класифицирање на производителите како високоризични. Нејасните и произволни критериуми за идентификување на производителите со висок ризик би можеле да доведат до дискриминаторски исклучувања, што потенцијално ќе им наштети на производителите од одредени земји кои не се членки на ЕУ, врз основа на непознати критериуми или фактори.Одредбата, исто така, поттикнува европски и меѓународни стандарди и технички спецификации за безбедноста на мрежните и информациските системи, но води кон потенцијални дискриминаторски практики. На производителите надвор од ЕУ им се налага да се борат со усогласување со специфичните стандарди кои се првенствено насочени кон ЕУ, односно се базирани на различна правна или регулаторна рамка. Ова може да доведе до исклучување на способни производители од други земји, иако нивните производи или услуги може да ги исполнуваат потребните технички и безбедносни критериуми. Дополнително, трошоците за усогласување со стандардите на ЕУ, исто така, може да бидат несразмерно високи за странските производители, што ги прави нивните производи поскапи или помалку конкурентни на пазарот во Република Северна Македонија.Имајќи го ова предвид, треба да истакнеме дека слободата на пазарот и претприемништвото е темелна вредност загарантирана со Уставот на Република Северна Македонија, а земјата треба да обезбеди еднаква правна положба на сите субјекти на пазарот.Ова се критични прашања кои мора да се решат за да се спречи прекумерна интервенција и да се осигури фер третман на производителите.**Препораки:**За да се одговори на овие проблеми, одредбата треба да се избрише или, алтернативно, може да се измени на следниов начин:* jасно да се дефинираат критериумите за „висок ризик“ врз основа на меѓународно признати стандарди и рамки за кибербезбедност;
* да се обезбеди јавна достапност на Регистарот, со процеси на донесување одлуки кои се транспарентни, одговорни и отворени за надворешна контрола;
* да се воспостави механизам за жалба за производителите кои сметаат дека неправедно се класифицирани како високоризични;
* да се утврди дека дискриминаторските практики засновани на политички или економски фактори се експлицитно забранети, одржувајќи неутралност во однос на технологиите во текот на имплементацијата на законот.
 |
| **Член 4, став 4**(4) Одредбите од овој закон се применуваат за образовните и научни установи што вршат критични и истражувачки активности. | Со Предлог Законот се предвидува дека истиот ќе се однесува и на образовните и научните установи што вршат критични и истражувачки активности.Сепак, оваа одредба е прилично нејасна и збунувачка од неколку аспекти:1. Недостаток на јасност: Одредбата е премногу широка и нема јасност во однос на нејзиниот опсег. Тоа го поставува прашањето дали се однесува на сите образовни институции или само на оние кои се занимаваат со критични и истражувачки активности. Формулацијата е двосмислена, бидејќи не е јасно дали образовните институции подлежат на законот само врз основа на нивните истражувачки активности или се вклучени сите образовни институции, без оглед на нивната вклученост во истражувањето. Оваа нејаснотија може да доведе до конфузија и неконзистентна примена на законот.
2. Неусогласеност со NIS2 Директивата: Одредбата не се усогласува со пристапот преземен од Директивата на ЕУ за безбедност на мрежи и информациски системи („**NIS2 Директива**“). NIS2 Директивата им остава на земјите членки да одлучат дали да ги применат нејзините одредби на образовните институции, особено кога тие спроведуваат критични истражувачки активности. Со проширувањето на одредбите од овој закон на образовните и научните институции, оваа одредба излегува надвор од опсегот на NIS2 Директивата, која не бара од земјите членки да наметнуваат такви обврски на образовните институции, освен ако тие конкретно не се сметаат за критични за мрежите и информациските системи.
3. Неусогласеност со дефиницијата за „*истражувачка организациј*а“: Според член 3 од Предлог Законот, „истражувачка организација“ се дефинира како „*субјект кој има примарна цел да спроведе применети истражувања или експериментален развој, со цел да се искористат резултатите од тоа истражување за комерцијални цели, но кој не ги опфаќа образовните институции*“. Од оваа дефиниција експлицитно се исклучени образовните институции. Така, предметната одредба, член 4 став 4, може да се смета за контрадикторна со наведената дефиниција, со оглед на тоа што, согласно оваа одредба, Предлог Законот ќе се однесува на образовните и научните институции кои вршат критична и истражувачка дејност.
4. Непотребно оптоварување на образовните институции: Вклучувањето на сите образовни и научни институции според одредбите на овој закон би наметнало непотребно оптоварување на институциите. Речиси сите високообразовни и научни институции се ангажирани во некоја форма на истражување, но не сите од нив би ги исполниле критериумите да бидат критични за националната безбедност или јавната безбедност. Подложувањето на истите законски барања како за организациите вклучени во критичната инфраструктура, може да резултира со прекумерни трошоци, административна комплексност и непотребно оптоварување на буџетот и операциите на образовните и научните институции.

Затоа, се препорачува оваа одредба да се преиспита или да се избрише, бидејќи непотребно го проширува опсегот на законот на образовните и научните установи кои не играат клучна улога во кибербезбедноста или националната безбедност. Треба да се усвои потаргетиран пристап, фокусирајќи се на институциите кои се директно вклучени во критичните активности и исклучувајќи ги образовните институции, освен ако тие не се конкретно вклучени во истражувачки активности кои ги исполнуваат критериумите да бидат критични за националната безбедност или јавната безбедност. |
| **Национално авторитативно тело за безбедност на мрежни и информациски системи** **Член 11 став 1****и****Национален центар за одговор на компјутерски инциденти** **Член 12 став 1** | Во овие два членови од Предлог Законот, забележителни се преклопувања во улогите поврзани со управувањето, анализата и известувањето за инциденти во однос на кибербезбедноста, и тоа:* И двата ентитета имаат задача да соработуваат, што потенцијално може да доведе до конфликтни или дуплирање на напорите при ангажирање на засегнатите страни.
* Улогата на MKD-CIRT е ограничена на „неговите сектори на одговорност“. Сепак, недостатокот на јасна дефиниција на овие сектори може потенцијално да се поклопува со општите одговорности на Министерството.
* Двата ентитета промовираат употреба на алатки и апликации за кибербезбедност со отворен код, што е вишок бидејќи не е јасно која е целната публика на секој ентитет.
* Двата ентитета организираат и спроведуваат обука за кибербезбедност и кампањи за подигање на свеста, при што фокусот на MKD-CIRT е специфичен за секторот. Меѓутоа, без јасна дефиниција на секторите, може да дојде до потенцијално преклопување во нивните улоги.

Двата субјекта се одговорни за донесување подзаконски акти кои се неопходни за спроведување на Предлог Законот. Ова уште еднаш може да предизвика дуплирање на напорите и преклопување или конкурентни прописи, што може да ја поткопа јасноста на правната рамка. Понатаму, разбираме дека Министерството има национална и постратешка улога, додека MKD-CIRT работи на секторско ниво. Така, подзаконските акти усвоени од овие две институции може ненамерно да се судираат или да се контрадикторни еден со друг (на пр. со пропишување различни стандарди или барања за мерки за кибербезбедност за исти субјекти). Без јасно разграничување на надлежностите, субјектите кои се во делокруг на Предлог Законот може да се соочат со потешкотии во практиката кои подзаконски акти треба да се следат. Наместо тоа, со Предлог Законот може да се назначи Министерството како единствен орган одговорен за донесување на подзаконските акти и со тоа и спроведување на законот, додека MKD-CIRT може да обезбеди технички податоци и препораки во текот на процесот на изготвување на подзаконски акти. |
| **Член 57**Законот за електронски документи, електронска идентификација и доверливи услуги, Законот за електронски услуги и електронско управување, Законот за централен регистар на население, Законот за електронските комуникации и Законот за енергетика ќе се усогласат со одредбите од овој закон во рок од две години од денот на влегување во сила на овој закон. | Со оглед на работите кои се уредуваат со Предлог Законот, како и фактот што некои аспекти се веќе уредени во други закони, двегодишниот период на усогласување на другите закони со одредбите од Предлог Законот може да предизвика правна несигурност за тоа кои одредби ќе се применуваат во одредени ситуации, бидејќи во моментов се во сила сите закони предвидени во овој член. |
| **Член 9 став 5**Ако субјектите од ставот (1) на овој член не постапат во согласност со одредбите на овој член, Министерството за дигитална трансформација е должно да ја извести Европската Комисија и ЕNISA, доколку се работи за субјект од земја членка на Европската Унија, а доколку се работи за субјект кој не е од земја членка на Европската Унија, Министерството за дигитална трансформација ќе ја извести соодветната држава, односно нејзиното надлежно тело за сајбер безбедност. | Терминот „ENISA“ првпат се употребува во овој член, без тој да биде соодветно дефиниран. Кратенката подоцна е дефинирана во член 25. Сметаме дека дефиницијата треба да се премести во член 9 став 5. |
| **Член 27, став 1, алинеја 7****-**придонесуваат за користење на алатки за безбедносна размена на информации во согласност со член 33 став (3) од овој закон. | Во член 33 нема став 3. Оваа одредба треба внимателно да се разгледа, а овој дел да се избрише или да се додаде став 3 во членот 33. |
| **Тимови за одговор на компјутерски инциденти (CSIRT)****Член 24 став 2**(2) Со посебните закони со кои се воспоставуваат секторски авторитативни тела може да се воспостават и секторски тимови за одговор на компјутерски инциденти за секторите од членот 4 ставови (2), (3), (4) и (5) од овој закон, а доколку со посебните закони не се воспостават вакви тела, надлежноста ја има Националниот центар за одговор на компјутерски инциденти во рамките | Членот 24 став 2 завршува со недовршена реченица. |
| **Член 3** | Во членот 3 (Дефиниции), по секоја дефиниција, употребата на точни интерпункциски знаци треба да се унифицира (со употреба на точка-запирка (;) по секоја дефиниција). |
|  | Забележавме многу правописни грешки низ текстот на Предлог Законот (на пр. зборот „*комјутер*“ наместо „*компјутер*“ како што е правилно, во неколку случаи низ текстот; „*се разменува информации*“ наместо „*се разменуваат информации*“ итн.). Предлог Законот треба внимателно да се разгледа за да се исправат сите правописни грешки. |
|  | Правилната македонска транскрипција на зборот „*сајбер*“ треба да се измени низ Предлог Законот („*кибер*“ наместо „*сајбер*“). |