|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Клаузули** | **Содржина** | **Предлог измена** | **Oбразложение** | **Релевантни линкови** |
| Член 187 | (3) Агенцијата во соработка со Националниот центар за одговор за компјутерски инциденти, треба да одреди критични компоненти и сензитивни делови од електронските комуникациски мрежи | (3) Агенцијата во соработка со националниот центар за одговор за компјутерски инциденти треба да одреди 5Г критични компоненти и сензитивни делови од електронските комуникациски мрежи, а врз основа на дефиницијата од ЕУ 5Г прирачникот за алатки. | 1. Агенцијата колку што е можно ќе ги земе предвид препораките насоки, мислења и методологии од Комисијата на ЕУ.  2. Целите н 5Г прирачникот служат за идентификација на можен заеднички сет на мерки кои се способни да ги ублажат главните ризици за сајбер безбедноста од 5Г мрежите, како и да обезбедат насоки за селекција на мерки кои би требало да бидат приоретизирани во ублажување на истите на национално ниво, како и на ниво на Унијата. **Од 5Г прирачникот (страна 39 и страна 40), јасно е наведено дека пристапната мрежа ,,RAN’’ и транспортот и трансмисионите функции не се сметаат за Критични функции.**  3. Од техничка перспектива, фактот дека имаме јасна поделба на пристапна мрежа ,,RAN’’ и јадро на 5Г. ,,RAN“ функционира како врска помеѓу мобилниот уред и основната мрежа и управува со целиот радио пристап за пренос на шифрирана рамнина на корисникот и контролна рамнина до основната мрежа. Оваа поделба на функции помеѓу ,,RAN’’ и ,,CORE’’ oвозомжува поефикасен развој на мобилни стандарди, каде што двете области може да се развијат независно, до одреден степен. Различни ,,RAN’’ може беспрекорно да работат меѓусебно со постоечкото јадро, користејќи стандардизирани интерфејси.  Ова ја подобрува отпорноста, ја поттикнува конкурентноста, а вклучително ја подобрува и безбедноста.  Ова е исто така  причината зошто оваа разделба ќе  остане еден од  клучните принципи во мобилните мрежи.  Од аспект на безбедност, раздвојувањето на ,,RAN’’, може да значи дека нејзиното работење не може да влијае на основната безбедност на мрежата. Оттука, 5Г јадрото, е местото каде што потребна е грижата од безбедносни причини. | Сајберсекјутирити на 5Г мрежите – ЕУ прирачник за ризици  https://digital-strategy.ec.europa.e  u/en/library/cyberse  curity-5g-networks-  eu-toolbox-risk-  mitigating-measures |
| Член 187 | (4) При проценка на ризиците за добавувачите и производителите за мрежна опрема, Агенцијата треба да ги земе во предвид следните фактори:  1. Дали добавувачите и производителите се под надзор на Владата на друга држава без независна судска контрола.  2. Дали добавувачите и производителите имаат јавно достапни информации за нивните основачи, деловни соработници, како и за управувачките и владеачките тела.  3. Дали добавувачите и производителите поддржуваат иновации, ги почитуваат авторските права и правата поврзани со нив, како и правата на интелектуална сопственост.  4. Дали добавувачите и производителите се транспарентно финансирани, во согласност со најдобрите практики за набавка на инвестиции склучување договори. | (4) При проценка на ризиците за 5Г добавувачите и 5Г производителите за мрежна опрема, Агенцијата треба да ги има во предвид  следните фактори:  1. Дали добавувачите и производителите се под надзор на Владата на друга држава без независна судска контрола.  2. Дали добавувачите и производителите имаат јавно достапни информации за нивните основачи, деловни соработници, како и за управувачките и владеачките тела.  3. Дали добавувачите и производителите поддржуваат иновации, ги почитуваат авторските права и правата поврзани со нив, како и правата на интелектуална сопственост.  4. Дали добавувачите и производителите се транспарентно финансирани, во согласност со најдобрите практики за набавка на инвестиции склучување договори.  5. Квалитет на производите на добавувачот и сајбербезбедносни практики, вклучувајќи контрола врз синџирот на производство како и тоа дали на безбедносните практики им е даден доволен приоритет.  6. Дали добавувачот има добиено сертификат за сајбербезбедност на ЕУ како што е NESAS.  7. Инциденти поврзани со сајбер безбедноста на добавувачите.  8. Дали добавувачот ги почитува прописите од областа на заштита на личните податоци. | 1.Наведувањето дека листата се однесува на електронските комуникациски мрежи 5G обезбедува безбедност за операторите кои моментално користат опрема за претходните генерации на технологии за широкопојасни мобилни мрежи и електронските комуникациски мрежи како целина, бидејќи нема да биде предмет на промена на целата опрема што моментално се користи и да направат дополнителни трошоци.  Наместо тоа, операторите ќе мора да ја осигураат безбедноста и безбедноста на новоимплементираната мрежна опрема 5G од самиот почеток.  **Ова е важно да се прецизира во насока на избегнување на ретроактивна примена на списокот, што би се сметало за противуставно бидејќи Уставот на република Северна Македонија гарантира дека законите и другите акти не можат да имаат ретроактивно дејство.**  2. Дополнително додадените 4 критериуми конкретно влијаат на користењето на опремата во однос на безбедноста. Бидејќи целта на нивното усвојување е ублажување на ризиците за безбедноста на мрежата, **има смисла да се додадат конкретни критериуми кои се фокусираат на проценка на нивото на заштита на добавувачите кои гарантираат за опремата и начинот на кој добавувачот работи како би бил усогласен со бројните безбедносни барања, вклучувајќи сајбер безбедност и заштита на податоците.**  Понатаму, првичните четири пропишани критериуми се чини дека немаат никаква врска со обезбедувањето на сајбер-безбедносна заштита на опремата и се поверојатно е да се толкуваат во политички контекст, со што се загрозува технолошката неутралност пропишана со Законот за електронски комуникации. **Со ставање на фокусот на сајбер-безбедносната заштита на опремата со додадените критериуми, помалку е веројатно дека Агенцијата ќе донесе одлука со која одредени добавувачи и даватели на мрежна опрема се означени како продавачи на значителен ризик поттикнат од било што друго освен опремата и технологијата што се користи.**  3. **Дефинирајќи дека мора да се исполнат повеќе од 5 критериуми за да може добавувачот или давателот на мрежна опрема да се смета за значително ризичен, гарантира дека добавувачите и давателите на мрежна опрема не се дискриминирани и исклучени поради неисполнување на еден од критериумите додека ги исполнуваат сите останати.** Ова е особено важно да се земе предвид ако добавувачите или добавувачите на мрежна опрема доаѓаат од земји каде што не се обврзани со регулативите на таа земја да исполнуваат некои од наведените критериуми (како што се нудат информации за нивните основачи или деловни соработници на јавноста). Земајќи во предвид дека Агенцијата мора да го почитува принципот на забрана за дискриминација и да ја заштити конкуренцијата, регулирајќи дека мора да се исполнат повеќе од 5 критериуми, обезбедува фер третман на добавувачите и давателите на мрежна опрема, особено со додадените критериуми за сајбер безбедност релевантни за оваа област.  4. Шемата за гаранција за безбедност на опремата на GSMA Network (NESAS) треба да ги олесни подобрувањата на нивоата на безбедност на опремата во мобилната индустрија, односно ќе доведе до обезбедување на една универзална и глобална безбедносна рамка. На крајот на краиштата, ќе доведе и до зголемување на довербата во мобилната мрежна опрема. | Шема за безбедност на мрежна опрема GSMA (NESAS)  https:gsma.com/security/network-equipment-security-assurance-scheme/ |
| Член 191 | Оператор во набавка на мрежна опрема  а) ..  б) ..  в) ..  г) да се земе предвид целокупниот ризик од влијание врз добавувачот и производителот од трета земја, особено во однос на:  - системот на управување  - постоењето на договори за безбедносна соработка или сродни договори, како што се одлуки за усогласеност во областа на заштитата на податоците.  - дали земјата е страна на мултилатерални меѓународни или билатерални договори за сајбер безбедност, борба против сајбер криминалот или заштита на податоците. | Оператор во набавка на мрежна опрема  а) ..  б) ..  в) .. | Kритериумите за оценување на добавувачите го нарушуваат принципот на еднаквост и се дискриминирачки. Земјата на потекло на добавувачот како критериум може да се користи како основа за дискриминација на добавувачите на хардвер или софтвер врз основа на нивното национално потекло.  Затоа, критериумите за проценка на ризикот треба да се ревидираат од перспектива на основниот законски принцип, особено во однос на:  **- Уставот на Република Северна Македонија**, според кој сите се еднакви пред законот, секој има право на еднаков третман од страна на јавните власти и никој не може да биде дискриминиран во политичкиот социјален или економски живот од која било причина.  - **Повелбата за фундаментални права на Европската Унија** која тврди дека сите се еднакви пред законот. Повелбата забранува каква било дискриминација врз основа на националност. Со ова, сегашните критериуми може потенцијално да го нарушат принципот на забрана за дискримација од член 20/21 од Повелбата за основните права на Европската унија.  - **Договорот меѓу Владата на РСМ и владите на другите земји се однесува на поттикнување и реципрочна заштита на инвестициите**, кој содржи општи стандардни заштитни клаузули за промоција, заштита и третман на инвестициите, гарантирајќи оправдување и правичен третман на инвеститорите од која било земја, не помалку поволен од третманот на инвестициите и поврзаните активности од страна на сопствените инвеститори или од страна на инвеститор од која било трета држава.  **- Општ третман на најповластена нација** (член 1 од ГАТТ) Принципот на третман на најповластена нација бара од членките на СТО да ги третираат сите други членки на СТО на ист привилегиран начин, исто така и Национален третман (член 3): Принципот на национален третман на ГАТТ обврзува Членките на СТО да ги третираат услугите и давателите на услуги слични странски и домашни производи подеднакво. Позициите заземени од АЕК ќе ја нарушат обврската за еднаков и фер третман со инвеститорите во Северна Македонија. Таквото прекршување може да биде основа за барања за отштета од инвеститори чии инвестиции во Северна Македонија ќе пропаднат како резултат на дискриминаторските политики на органите на јавната администрација. |  |
| Член 187 | (1) Агенцијата во соработка со Националниот центар за одговор на компјутерски инциденти периодично подготвува детална проценка на профилот на ризик на национално ниво на сите релевантни добавувачи и производители на мрежна опрема кај операторите. | (1) Агенцијата во соработка со Националниот центар за одговор на компјутерски инциденти периодично подготвува детална проценка на профилот на ризик на национално ниво на сите релевантни 5 G добавувачи и производители на мрежна опрема кај операторите. а оваа проценка ќе ја договорат Министерството за информатичко општество и администрација, Mинистерството за економија, Mинистерството за правда, Mинистерството за надворешни работи, Mинистерството за внатрешни работи и други сродни органи. | 1. Проценката на добавувачот и исклучувањето на одреден добавувач дефинитивно ќе влијае на интересот на пошироката јавност што на долг рок може да влијае на **националната економија, владиниот буџет и технолошкиот напредок, пазарот на електронски комуникации** и долгорочно може да **влијае на билатералните деловни односи помеѓу компании од Република Северна Македонија и други земји, како и процесот на пристапување во ЕУ како земја-членка. Исто така, долгорочно влијае врз правниот систем на државата и заштитата на човековите права и слободи**.  2. Земајќи референца од добрата правна практика, како пример од Германија, **Министерството за внатрешни работи може да забрани употреба на критична компонента во** **однос на операторот на критичната инфраструктура** ВО **ДОГОВОР СО ЗАСЕГНАТИТЕ МИНИСТЕРСТВА (Економија, Надворешни работи работи)** во рок од еден месец од приемот на известувањето за критичната компонента или издаваат наредби: Доколку ,,преовладувачките јавни интереси“, особено загриженоста за безбедносната политика на Сојузна Република Германија, стојад против нивната употреба. | Закон за ИТ безбедност на Германија 2.0  [https://www.gestze-imnternet.de/bsig 2009/BJNR282110009.html](https://www.gestze-imnternet.de/bsig%202009/BJNR282110009.html) |