Приложение № 1 към Решение № 162/19.05.2022 г.

БЕЛЕЖКИ НА ЗАИНТЕРЕСОВАНИТЕ ЛИЦА ПО ПРОЕКТ НА ПРАВИЛА ЗА МИНИМАЛНИТЕ ИЗИСКВАНИЯ ЗА СИГУРНОСТ НА ОБЩЕСТВЕНИТЕ ЕЛЕКТРОННИ СЪОБЩИТЕЛНИ МРЕЖИ И УСЛУГИ И МЕТОДИ ЗА УПРАВЛЕНИЕ НА РИСКА ЗА ТЯХНАТА СИГУРНОСТ (ОБЩЕСТВЕНИ КОНСУЛТАЦИИ, ОТКРИТИ С РЕШЕНИЕ № 81/10.03.2022 г. НА КРС)				
№	**ЗАИНТЕ-РЕСОВАНО ЛИЦЕ**	**СТАНОВИЩЕ**	**СТАТУС**	**МОТИВИ**
ОБЩИ БЕЛЕЖКИ				
1.	**„А1 БЪЛГАРИЯ“ ЕАД (А1)**	На интернет страницата на Комисията за регулиране на съобщенията (КРС) е публикуван за обществено обсъждане проект на „Правила за минималните изисквания за сигурност на обществените електронни съобщителни мрежи и услуги и методи за управление на риска за тяхната сигурност. „А1 България“ ЕАД (А1), заедно с другите предприятия, предоставящи електронни съобщителни мрежи и/или услуги в страната имаше възможност да участва в работните групи по подготовката на документа, което считаме за изключително важно и видно от публикувания проект, е дало добри резултати.		В становището се подкрепя подхода на Комисията за регулиране на съобщенията (КРС/Комисия) за създаване на работна група при изготвянето на проекта на Правила за минималните изисквания за сигурност на обществените електронни съобщителни мрежи и услуги и методи за управление на риска за тяхната сигурност (проект на Правила).
2.	**МИНИСТЕРСТВО НА ВЪТРЕШНИТЕ РАБОТИ**	По публикувания от КРС проект на Правила за минималните изисквания за сигурност на обществените електронни съобщителни мрежи и услуги и методи за управление на риска за тяхната сигурност, от страна на		Становището подкрепя проект на Правила на КРС.

		МВР няма забележки.		
3.	**МИНИСТЕРСТВО НА ОТБРАНАТА НА РЕПУБЛИКА БЪЛГАРИЯ**	Във връзка с открита процедура за обществено обсъждане на разработения съгласно чл.243, ал. 3 на Закона за електронни съобщения, проект на Правила за минималните изисквания за сигурност на обществените електронни съобщителни мрежи и услуги и методи за управление на риска за тяхната сигурност, Министерство на отбраната няма възражения и предложения по текста на проекта.		Становището подкрепя проект на Правила на КРС.
4.	**„ЦЕТИН БЪЛГАРИЯ“ ЕАД (ЦЕТИН)**	Считаме че така представеният Проект е в съответствие с чл. 243, ал. 3 от ЗЕС, както и е съобразен с изискванията на приложимите актове на Европейската комисия и отчита в максимална степен препоръките, насоките, становищата, общите и добрите практики и методологии на ENISA. В Проекта са включени всички предложения на ЦЕТИН, приети в хода на работата на двата Консултативни съвета по въпросите на сигурността на обществените фиксирани и мобилни електронни съобщителни мрежи и услуги, създадени в Решения №№ 425/17.12.2020 г. и 34/28.01.2021 г. В заключение, ЦЕТИН приветства така представения Проект, като отчита неговата важност за подобряването на сигурността и правилното управление на риска за		Становището подкрепя проект на Правила на КРС.

		електронните съобщителни мрежи и услуги. Допълнително изказваме своята благодарност към Комисията за конструктивната работа, като се надяваме тя да продължи и по други регулаторни въпроси в бъдеще.		
Постъпили становища по Глава втора от проекта на Правила				
5.	**Григор Ваклинов**	В чл.6, ал.2 вероятно поради техническа грешка е записано, че „се определят ... отговорностите на лицата, извършващи оценката“, а не отговорностите на лицата, които ще се справят с потенциалните заплахи и последиците от тях. В повечето случаи лицата извършващи оценката ще са различни от лицата, които ще се справят със заплахите. Вероятно се имат предвид например някои от отговорните лица, посочени в чл.9.	**НЕ СЕ ПРИЕМА**	Няма допусната техническа грешка в чл.6, ал.2. Правилата се отнасят до широк кръг от предприятия, предоставящи различни обществени електронни съобщителни мрежи и/или услуги, които се различават организационно и като структура на управление. В тази връзка, КРС дава възможност лицата по чл.6, ал.2 да са различни в общия случай от лицата по чл. 9.
6.	**А1**	В чл. 7 следва да се направи корекция, така че да отпадне изискването за описване на активи на „трети страни“, а в списъка да се включват само активи, които са собствените на компанията. Стандартният начин за оценка на риска включва управление на собствени ресурси (ресурси под наш контрол). Контролът върху доставчици се осъществява през споразумения за SLA/сигурност/защита на данните и не описва/инвентаризира пряко активите, с	**НЕ СЕ ПРИЕМА**	Съгласно чл. 243, ал. 3 второ изречение от Закона за електронни съобщения (ЗЕС) при определянето на Правилата комисията се съобразява с изискванията на приложимите актове на Европейската комисия и отчита в максимална степен препоръките, насоките, становищата, общите и добрите практики и методологии на Агенцията на Европейския съюз за киберсигурност, както и приложимите европейски схеми за сертифициране на киберсигурността, установени с актове на Европейската комисия, и приложимите европейски и международни стандарти

		които се осъществява дейността на поддоставчика. На практика, описването на активи, които са чужда собственост и са под чужд контрол ще е изключително трудно, ако не и невъзможно за предприятията.		и стандартизационни документи. Съгласно т.4.1 от Насоките на ENISA за мерките за сигурност, съгласно Европейския кодекс за електронни съобщения (Насоките на ENISA за мерките за сигурност)[1], мерките се отнасят до всички активи на предприятието (включително относимите активи на „трети страни“). В тази връзка е уточнено, кои са относимите активи, а именно тези които при компрометиране или отпадане могат да предизвикат инцидент, свързан със сигурността на мрежата и/или услугата. Текстът в проект на Правила съответства на Насоките на ENISA за мерките за сигурност.
7.	**Григор Ваклинов**	За по-добра подреденост и яснота е подходящо второто изречение на чл.7, ал.4 „Под „трети страни“ не се разбират ползватели на услугите и държавни или регулаторни органи.“ да се отдели в отделна алинея пета на същия член.	**ПРИЕМА СЕ**	По мотивите в становището на г-н Григор Ваклинов.
8.	**Григор Ваклинов**	В чл.8 думата „издържат“ е подходящо да се замени с някоя по-подходяща дума като „осигуряват“, „поддържат“ или „притежават“. Според определението в § 1, т. 4 „Нивото на сигурност е способността…“, а способността не се издържа, а се осигурява, поддържа или притежава.	**НЕ СЕ ПРИЕМА**	Съгласно § 1, т. 63 от ДР на ЗЕС за „сигурност на електронните мрежи и услуги е способността на електронните съобщителни мрежи и услуги да **издържат** …**“**. Думата *„издържат“* се отнася до електронните съобщителни мрежи и услуги, а не до способността. В тази връзка, КРС счита, че трябва да се придържа към легалната дефиниция.

[1] Guideline on Security Measures under the EECC https://www.enisa.europa.eu/publications/guideline-on-security-measures-under-the-eecc, стр.: 15: Third parties and third party assets are in scope just as if they were assets of the providers. In other words, even if certain processes are outsourced, the provider remains responsible for ensuring that appropriate security measures are taken to protect the security of networks and services it is providing.

9.	**Григор Ваклинов**	Текстът на чл.13, ал.4 трябва коренно да се промени или да отпадне, защото е спорно от юридическа, а и от практическа гледна какви точно санкции и в какъв размер могат да се определят в договорни отношения с доставчик на оборудване, което „би могло да доведе до неизпълнение на задължения по настоящите правила“. От една страна имаме една вероятност на събитието, отразена в израза „би могло да доведе“, а от друга страна как ще се определи степента на вината на доставчика?	**НЕ СЕ ПРИЕМА**	Съгласно стратегическа мярка 3 на от Инструментариума на ЕС за киберсигурността[2] на мобилните оператори трябва да бъде осигурена възможност да контролират доставчиците на оборудване на базата на оценката на техния рисков профил. В тази връзка, КРС счита че залагането на санкции за неизпълнение в договорите са подходящ механизъм за изпълнение на мярката и обезпечаване на точното им изпълнение от страна на доставчиците на оборудване. Използването на думите „би могло да доведе до неизпълнение на задълженията по настоящите правила“ сочи, че санкциите за неизпълнение на договорите между предприятията и техните доставчици на оборудване не са при условие, че са довели до нарушение на подзаконовия нормативен акт, а с прилагат независимо от евентуалната отговорност за предприятията, реализирана по административен ред. По отношение на въпроса за вината на доставчика, въпросът е от договорен характер и извън обхвата на обсъждания подзаконов нормативен акт.
10.	**Григор Ваклинов**	В чл.14, ал.3 думата „разговор“ е подходящо да се замени с „анкета“ или „беседа“.	**НЕ СЕ ПРИЕМА**	В посочената разпоредба КРС цели да обърне внимание, че одита не представлява само преглед на документи, а също така и в неформален диалогичен вид. Подобен принцип е заложен в серия стандарти ISO 27000 (Системи за управление на информационната сигурност). В допълнение считаме, думата *„разговор“* за най-подходяща, защото представлява *устна* размяна на информация (диалог)

[2] Cybersecurity of 5G networks EU Toolbox of risk mitigating measures https://ec.europa.eu/commission/presscorner/detail/en/qanda_20_127

				между двама или повече участника за постигане на съгласие по някакъв въпрос, в конкретния случай, между лицето, извършващо одит и отговорните служители. Думата *„анкета“* се използва за събиране на необходимата информация в писмена форма и по предварително формулирани въпроси, а думата *„беседа“*, нищо че е синоним на *„разговор“*, често се използва и за изказване на едно лице пред голяма аудитория без възможност за отговор.
Постъпили становища по Глава втора от проекта на Правила				
11.	**А1**	Предлагаме чл. 22, ал. 3 да отпадне. Считаме, че всички следва да се докладват само при критериите от Приложение № 2 към правилата. Няма ефективен способ за комуникация между предприятията, който да е подходящ от гледна точка на конкуренцията. Задължението ще означава постоянен обмен на техническа информация между всички предприятия в страната, като част от тази информация определяме като чувствителна.	**ПРИЕМА СЕ ЧАСТИЧНО**	Разпоредбата на чл. 22, ал. 3 не е нова, изискването за докладване на такива инциденти съществува в Общите изисквания при осъществяване на обществени електронни съобщения от 2012 г. Текстът се отнася за случаите, когато инцидент възникнал в мрежата на едно предприятие засяга нормалната работа и предоставянето на услуги в мрежи на други предприятия. В тези случаи предприятието, което отдава електронна съобщителна мрежа ще знае, че са засегнати и други предприятия, както и предприятието, което ползва чужда електронна съобщителна мрежа ще знае, че я използва. За да не се налага обмен на техническа или друга информация между отделните предприятия е направеното изключение и за тези инциденти се докладва без да е необходимо да се прави оценка на засегнатите ползватели. За подобен тип инциденти оценката може да бъде направена само от КРС, като получи информация от всички предприятия. КРС приема, че с цел яснота е редно цитираната

				разпоредба да бъде преместена в чл. 24, като нова т. 5 и променена в следния вид: „*инцидентът засяга функционирането мрежите и/или услугите на няколко предприятия*“. По този начин разпоредбата е на систематичното си място, при качествените критерии за докладване на инциденти и същевременно е ясно, че не се изисква обмен на информация между различни предприятия.
12.	**А1**	Чл. 23 следва да се промени и да придобие следната редакция: „*Чл. 23. Количествен критерий за инцидент, свързан с автентичността, целостта или поверителността - съгласно Приложение № 2.*“. Считаме, че критериите за уведомление при инциденти следва да са тези, посочени в Приложени 2 към правилата. Не виждаме причина в основния текст на наредбата да се изнася отделен количествен критерий. Така се създава потенциал за неяснота при тълкуване и прилагане на текстовете.	**ПРИЕМА СЕ**	Съгласно мотивите на А1.
Постъпили становища по проектите на Приложения към Правилата				
13.	**А1**	В Приложение № 1 към чл. 10, ал. 1 „Технически и организационни мерки за сигурност“, таблица Област на сигурност 6: Управление на непрекъсваемостта, Цел на сигурност 22: Способност за възстановяване при бедствия, в т. 1, колона 3 е използвано понятието „отказоустойчиви сайтове“, което считаме за неясно. Молим същото да се	**ПРИЕМА СЕ**	Съгласно мотивите на А1, текста придобива вида: *„Съществуват мерки за справяне с бедствия, като резервирани елементи на мрежата в други региони, архивиране на критични данни на отдалечени места и т.н.“*

		прецизира, така че да е възможно предприятията да разбират и изпълнят изискването.		
14.	**А1**	Предлагаме промяна в Приложение 2 за фиксирана гласова услуга, фиксиран достъп до интернет, междуличностна съобщителна услуга без номер и услуги за разпространение на радио- и телевизионни програми, доколкото смятаме, че следва да се направи разделение по отношение на праговете за докладване на инциденти, както следва: 1. За предприятия с до 50 000 абоната на фиксирани услуги; 2. За предприятия с над 50 001 абоната: За първата категория: Брой ползватели, засегнати от инцидента Продължителност на инцидента >= 35 000 >= 1 час >= 25 000 >= 2 часа >= 10 000 >= 4 часа >= 5 000 >= 6 часа >= 1 000 >= 8 часа За втората категория: Брой ползватели, засегнати от инцидента Продължителност на инцидента >= 250 000 >= 1 час >= 150 000 >= 2 часа >= 100 000 >= 4 часа	**НЕ СЕ ПРИЕМА**	Съгласно чл. 243, ал. 3 второ изречение от Закона за електронни съобщения (ЗЕС) при определянето на Правилата комисията се съобразява с изискванията на приложимите актове на Европейската комисия и отчита в максимална степен препоръките, насоките, становищата, общите и добрите практики и методологии на Агенцията на Европейския съюз за киберсигурност, както и приложимите европейски схеми за сертифициране на киберсигурността, установени с актове на Европейската комисия, и приложимите европейски и международни стандарти и стандартизационни документи. Съгласно Насоките на ENISA за докладване на инциденти[3] праговете за докладване на инциденти се определят от регулатора отчитайки общия брой ползватели на услугата на национална база, а не броя на конкретното задължено предприятие. Диференцираният подход спрямо различните предприятия е базиран на Насоките на ENISA за мерките за сигурност. Разликата в Насоките на ENISA не е случайно, в първия случай се цели съизмеримост на различните инциденти оказали значително въздействие, докато мерките за сигурност се предприемат спрямо конкретната мрежа или услуга на всяко различно предприятие. Доколкото е необходимо отчитане на обема на дейността на отделните предприятия, това намира отражение в

[3] Technical Guideline on Incident Reporting https://www.enisa.europa.eu/publications/enisa-technical-guideline-on-incident-reporting-under-the-eecc

		>= 50 000 >= 6 часа >= 10 000 >= 8 часа Основните ни мотиви за това са свързани с значителния брой на предприятията, предоставящи телевизия и достъп до интернет, от една страна и консолидацията в тези сегменти, в следствие на която са налице ограничен брой предприятие с по-голям пазарен дял на национално ниво. По този начин критериите ще отговарят на развитието на пазара на фиксирани услуги в страната. Важно е да отбележим, че същия критерий (50 000 абоната) е използван от КРС в чл. 12 от Проекта на Правила и логично е да се приложи и за Приложение 2 за фиксирани мрежи и услуги.		определените прагове в проекта. Предложението на А1 отчита структурата на пазара, но приемането му ще доведе до ситуация, в която в КРС ще постъпва информация единствено от предприятията с под 50 000 абоната за инциденти засягащи значителен брой абонати, които няма да се нотифицира, ако доставчикът има над 50001 абоната. Подобен подход ще лиши комисията от информация за инциденти, засягащи голям брой абонати в мрежите на водещите оператори, което не отговаря на целите, които се поставят със събирането на информацията.