С П Р А В К А

ЗА ОТРАЗЯВАНЕ НА ПОСТЪПИЛИТЕ ПРЕДЛОЖЕНИЯ ОТ ОБЩЕСТВЕНИТЕ КОНСУЛТАЦИИ ПО ПРОЕКТ НА РЕШЕНИЕ НА МИНИСТЕРСКИЯ СЪВЕТ ЗА ОДОБРЯВАНЕ НА ПРОЕКТ НА ЗАКОН ЗА ИЗМЕНЕНИЕ И ДОПЪЛНЕНИЕ НА ЗАКОНА ЗА КИБЕРСИГУРНОСТ

Организация/потребител (вкл. начина на получаване на предложението)	**Бележки и предложения**	**Приема/не приема предложението**	**Мотиви**
Iliya Hristozov	Така предложеният текст на разпоредбата на **§ 42, т. 1 от проекта:** *§ 42. В Закона за електронните съобщения се правят следните изменения и допълнения:* *1. В чл. **16**, се създава **ал. 2а**:* *„**(2а)** Национален компетентен орган за субектите по чл. 4, **ал. 1,** т. 3, буква а) и б) е Комисията за регулиране на съобщенията.“* е неточен и непълен, защото е ясно, че не може да става въпрос за чл. 16 от ЗЕС, който регламентира дейностите на министъра на транспорта и съобщенията, а и няма алинеи в него. Освен това, така написана в ЗЕС, тази разпоредба реферира към разпоредбите на чл. 4, ал. 1, т. 3, буква а) и б) от ЗЕС, но в тях не става въпрос за субекти, а за целите на закона. Един внимателен анализ показва, че вероятно се имат предвид изменените разпоредби на чл. 4, т. 3, буква а) и б) от самия Закон за киберсигурност. За преодоляване на горепосочената грешка, **предлагам разпоредбата на § 42, т. 1 от проекта да се измени в един от двата варианта:** Вариант **1**: *1. В чл. 21 се създава ал. 6:* *„(6) Комисията изпълнява функциите на национален компетентен орган за субектите по чл. 4, т. 3, буква а) и б) от Закона за киберсигурност.“*	**Приема се**	

	или Вариант **2:** *1. В чл. 30, ал. 1 се създава т. 30:* *„30. изпълнява функциите на национален компетентен орган за субектите по чл. 4, т. 3, буква а) и б) от Закона за киберсигурност.“* в зависимост от това, за кое място в ЗЕС се прецени, че е по-подходящо за тази разпоредба.		
Iliya Hristozov	Вероятно горепосочената грешка в разпоредбата на § 42, т. 1 от проекта се е допуснала, защото на някакъв по-ранен етап от изготвянето на проекта, тази разпоредба е била предвидена като нова алинея 2а на чл. 16 от самия Закон за киберсигурност, **в което също има логика и смисъл**. Затова, ако се прецени, че е необходимо, **предлагам да се добави като § 17, т. 3 от проекта разпоредбата във вида:** *3. В чл. 16 се създава ал. 2а:* *„(2а) Национален компетентен орган за субектите по чл. 4, т. 3, буква а) и б) е Комисията за регулиране на съобщенията.“* и следващите точки в § 17 да се преномерират.	**Приема се.**	
Iliya Hristozov	**1.** На много места в изменените разпоредби на закона се правят препратки към „*чл. 4, **ал. 1**, т….*“, но в изменения текст на разпоредбата на чл. 4 вече няма алинеи, а само точки. Затова **предлагам тези препратки да се коригират на** „*чл. 4, т….*“.	**Приема се.**	
Iliya Hristozov	**2.** Предлагам в разпоредбата на § 17, т. 3, буква е) от проекта **думите „***т. 6 и 7***“ да се заменят с думите „***т. 6, 7 и 8***“**, защото се създава и нова т. 8.	**Приема се.**	
Iliya Hristozov	**3.** Предлагам **разпоредбата на § 40, т. 1 от проекта да се измени във вида:** *„1. в срок до три месеца от влизането в сила на закона определя с решение административните органи по чл. 16, ал. 1 и приема методиката по **чл. 16, ал. 3, т. 8**;“*	**Приема се.**	

	защото приемането на тази методика вече ще е регламентирано в чл. 16, ал. 3, т. 8 от закона.		
Iliya Hristozov	**4.** Предлагам в разпоредбата на § 41 от проекта **думите „***решението по § 41, т. 1***“ да се заменят с думите „***решението по § 40, т. 1***“** за да е точна препратката.	**Приема се.**	
Iliya Hristozov	**5.** За по-добра прецизност **предлагам разпоредбата на § 42, т. 2 от проекта да се измени във вида:** *„2. В чл. 30, ал. 1, т. 22 думите „като при необходимост си съдейства с компетентните органи по чл. 244а, ал. 3“* ***и запетайката пред тях*** *се заличават.“*	**Приема се.**	
Iliya Hristozov	**6.** В разпоредбата на § 42, т. 4 от проекта предлагам да се коригира думата „*петнад**а**сета*“ с думата „*петнадесета*“.	**Приема се.**	
nipetkov	Бих искал да обърна внимание на частта ОТ (Оперативни Технологии), които са от съществено значение за производствените предприятия. По своята същност ОТ се различават значително от ИТ, като тук специалистите по темата „Киберсигурност“ трябва същевременно да разбират в детайли и темата „Системи за Индустриална Автоматизация“. Изискванията и добрите практики към ОТ са описани в стандарта **IEC 62443**, който покрива част от стандарта **ISO 27000** и от стандартите **IEC 61511 / IEC 6150**8 по отношение на функционалната сигурност. Този стандарт условно може да се раздели на три подраздела, които посочват различните изисквания, а именно: Подраздел отнасящ се към крайните потребители (Производствените предприятия), които са обект на проверка съгласно МИС2; Подраздел отнасящ се към фирмите Системи Интегратори (проектантски и инженерингови фирми), които проектират и внедряват Системи за Автоматизация и Задвижванията при горните; Подраздел отнасящ се към производителите на технологично оборудване, занимаващи се с развойна дейност и производство на софтуерни и хардуерни продукти.	**Приема се по принцип.**	

	Както при ИТ, така и при ОТ обследването на съществуващата ситуация съгласно изискванията на IEC 62443 е началото на процеса по оценка на актуалното нивото сигурност, определящо последващите мерки за преминаване към по-високо ниво на сигурност. Това са само част от особеностите в частта ОТ, поради което препоръчвам при производствените предприятия да се обърне допълнително внимание на оценката на частта ОТ.		
MPA	The Motion Picture Association (MPA) служи като глобален глас и защитник на международната филмова, телевизионна и стрийминг индустрия. Наши членове са Walt Disney Studios Pictures, Netflix Studios, LLC, Paramount Pictures Corporation, Sony Pictures Entertainment Inc., Universal City Studios LLC и Warner Bros. Discovery. Компаниите, членуващи в MPA, продуцират и инвестират значителни средства в производството на европейско аудиовизуално съдържание, което намира и глобална аудитория чрез тяхното разпространение. MPA играе водеща роля в борбата с незаконното разпространение на защитено съдържание, което вреди на развитието на дигиталната екосистема. Целта на MPA е да намали и овладее ефектите от пиратството чрез ефективни стратегии за правоприлагане, насочени към операторите на незаконни сайтове и услуги, както и към посредниците, които предоставят технически условия за тяхната дейност. MPA приветства предприетите действия по транспониране на преработената Директива относно сигурността на мрежовите и информационните системи (Директива NIS2), и по-специално разпоредбите на член 28 и съображения 109-112, свързани с услугите за регистрация на домейни. Осигуряването на достъп до надеждни данни за регистрантите ("WHOIS данни") е от съществено значение за борбата с незаконното и вредно съдържание онлайн, включително съдържанието, нарушаващо авторските права, и за защитата на здравето и сигурността на гражданите. Следва да се отбележи, че проучването на Европейската комисия относно злоупотребите с DNS от 2022 г. посочва проверката на данните от WHOIS като една от основните		

	препоръки за предотвратяване, откриване и намаляване на злоупотребите с DNS. Европейската комисия също така неотдавна призна в Препоръката за борба с фалшифицирането от 2024 г., че "точността и пълнотата на данните за регистрация на име на домейн също може да играе централна роля при прилагането на правата върху интелектуалната собственост", като допълнително подчерта необходимостта предоставените данни за регистрация да бъдат точни, проверени и да се отнасят до действителния ползвател на името на домейна, а не просто до доставчик на услуги за защита на личните данни или прокси. По изложените причини приветстваме възможността да представим нашите коментари относно българския проектозакон и по-специално нашите опасения относно изключително ограничения обхват на проекта на член 27в алинея 4.		
MPA	**Становище по прилагане на Директивата NIS2: постигане на целта на член 28 за публичен достъп до надеждна информация за WHOIS (част 2)** По-долу са посочени следните приоритети и препоръки за осигуряване на адекватно прилагане на член 28 и съображения 109-112 от Директива NIS2 и за значително увеличаване на достъпността и точността на данните от WHOIS: **Лица, законно търсещи достъп и данни**: Съображение 110 дефинира "законно търсещия(ите) достъп" до данните от WHOIS по смисъла на член 28 параграф 5 от Директива NIS2 като "всяко физическо или юридическо лице, което отправя искане съгласно правото на Съюза или националното право". Настоятелно призоваваме българският законодател да преразгледа обхвата на член 27в алинея 4, който е изключително тесен и задължава регистрите на имена на домейни от първо ниво (TLD/ДПН) и организациите, предоставящи услуги по регистрация, да си сътрудничат само с националните компетентни органи и органите на досъдебното производство. Обхватът следва да бъде разширен, така че да включва и всяко физическо или юридическо лице, което отправя искане за достъп до данни	**Не приема предложението.**	Съображение 110 от Директива (ЕС) 2022/2555 включва обяснение на понятието "законно търсещия(ите) достъп", което да послужи за разпоредбата на член 28, като законодателя не прилага официална дефиниция на горецитираното понятие. С други думи легална дефиниция на съществува по смисъла на член 2 от Директива (ЕС) 2022/2555. Подобно разширително тълкуване на нормата би довело до създаване на огромен обем от

	от WHOIS с цел разследване на правонарушение, включително, без ограничение, за установяване, упражняване или защита на киберсигурност, интелектуална собственост, защита на потребителите или други правни претенции в качеството си на лице, "законно търсещ(и) достъп". Това разширяване на кръга легитимирани лица е от решаващо значение за осигуряването на достъп до конкретни данни за регистрация на имена на домейни при законни и надлежно обосновани искания. Описаното съответства с наскоро публикуваната препоръка на Европейската комисия относно борбата с фалшифицирането, която насърчава субектите, предоставящи услуги по регистрация на имена на домейни в ЕС, да признават всички физически или юридически лица, които отправят искане за право на информация (ROI) съгласно Директива 2004/48/ЕО относно упражняването на права върху интелектуалната собственост (IPRED), за лица, законно търсещи достъп. Въз основа на изложеното предлагаме настоящата редакция на член 27в алинея 4 да бъде изменена така, че да задължи регистрите на имена на ДПН и организациите, предоставящи услуги за регистрация на имена на домейни, да сътрудничат на законно търсещите достъп, което следва да включва *всяко физическо или юридическо лице, което подава искане за достъп до данни от WHOIS за разследване на правонарушение, включително, без ограничение, за установяване, упражняване или защита на киберсигурност, интелектуална собственост, защита на потребителите или други правни претенции.* Освен това достъпът до данни от WHOIS съгласно съображение 112 от Директива NIS2 трябва да бъде безплатен и тези данни трябва да се предоставят при поискване от законно търсещия достъп без неоправдано забавяне.		задължения за регистрите на имена на домейни от първо ниво и субектите, предоставящи услуги за регистрация на такива имена на домейни. Методът на транспониране на Директива (ЕС) 2022/2555 на Европейския парламент и на Съвета от 14 декември 2022 година относно мерки за високо общо ниво на киберсигурност в Съюза, за изменение на Регламент (ЕС) № 910/2014 и Директива (ЕС) 2018/1972 и за отмяна на Директива (ЕС) 2016/1148 (Директива МИС 2), който е възприет и съгласуван от Р България е на минимална хармонизация, относно прилагането на горецитираните текстове. Съответо субектите имащи право на достъп до конкретна информация се обективират изрично в преамбюл 110, а именно: „Те могат да включват органи, които са компетентни съгласно

			настоящата директива, и органи, които съгласно правото на Съюза или националното право са компетентни за предотвратяването, разследването, разкриването или наказателното преследване на престъпления, както и CERT или ЕРИКС.“ В текста от проекта на закона за изменение и допълнение на закона за киберсигурност (ЗИД на ЗКС), а именно „База данни с регистрационни данни на имена на домейни - Чл.27в (4) *Субектите по ал. 1 са длъжни да оказват съдействие на националните компетентни органи, СЕРИКС, НЕРИКС и органите на досъдебното производство, като предоставят, в срок до 72 часа, достъп до конкретни данни за регистрация по ал. 2, при наличие на обосновано и законосъобразно искане и в съответствие с приложимото право в*

			областта на защитата на личните данни.“ се задава ясна дефиниция на процеса по разкриване на информация, отговорните органи и срокове за изпълнението им, техните правомощия, както и задължението на регистрите на имена на домейни от първо ниво и субектите, предоставящи услуги за регистрация на такива имена на домейни за разкриване на конкретна информация.
	Бихме искали да обърнем внимание на неотдавнашното белгийско транспониране, което включва "**всяко лице в контекста на нарушения на права върху интелектуална собственост или сродни права**" в списъка на лицата, които се считат за лица, законно търсещи достъп за целите на исканията за предоставяне на достъп до данни за регистрация на имена на домейни. Ето защо, с уважение насърчаваме българските власти да приложат подобен подход, за да се даде възможност за ефективно наблюдение и борба с незаконните дейности онлайн.		Регулация в Р България, която касае правото на интелектуалната собственост от години съществува в специални закони като: Закон за авторското право и сродните му права, Закон за патентите и регистрацията на полезните модели, Закон за марките и географските означения, Закон за промишления дизайн и т.н. В посочената нормативна база ясно съществуват разписани правила и процедури относно защитата на

			интелектуалната собственост, процедирането и защитата на различните видове граждански права.
	Третиране на въпроса за използването на прокси услуги/ услуги за защита на личните данни: В проучване на Службата на ЕС за интелектуална собственост (EUIPO) от 2021 г. се отбелязва, че "значителен процент от имената на домейни, използвани за извършване на незаконни или вредни дейности в интернет, са регистрирани чрез услуги за защита на личните данни или прокси услуги" и че след влизането в сила на Общия регламент за защита на данните обосновката на законното използване на услуги за защита на личните данни или прокси услуги "е поставена под въпрос".		Липсва предложение.
MPA	**Становище по прилагане на Директивата NIS2: постигане на целта на член 28 за публичен достъп до надеждна информация за WHOIS (част 3)** Поради това при транспонирането на Директива NIS2 на национално равнище трябва да се вземе предвид популярността на услугите за прокси сървъри или за защита на личните данни сред лицата, извършващи незаконни и вредни дейности онлайн. Когато се подава законно искане за достъп, трябва да се разкрият основните данни на действителния клиент/ползвател на името на домейна, а не само данните на доставчика на услугата за защита на личните данни или прокси услугата, ако такава услуга за защита на личните данни или прокси услуга е била използвана в процеса на регистрация. Ето защо приветстваме факта, че в българския проектозакон се пояснява, че понятието "доставчик на услуги за регистрация на имена на домейни" следва да се разбира като обхващащо доставчиците и препродавачите на услуги за защита на личните данни и прокси услуги. Въпреки това бихме препоръчали също така проектозаконът да включва изрично следната формулировка при прилагането на член 28 от Директивата NIS2: "*При предоставянето на данни в отговор на законни искания за достъп регистрите на имена*	**Не приема предложението.**	Изискванията на Директивата са транспонирани с разпоредбата на чл.27в. Следва да се отбележи, че министърът на електронното управление няма правомощия в областта на разследвне и предотвратяване на компютърни престъпление, материята е предмет на Наказателния кодекст и приложимото законодателство.

	на ДПН и организациите, предоставящи услуги за регистрация на имена на домейни, предоставят данните на действителния ползвател на името на домейна и не могат да предоставят вместо това данните на доставчика на услуги за защита на личните данни или данните на доставчика на прокси услуги за регистрация, които може да са били използвани в процеса на регистрация на името на домейна." **Третиране на въпроса за предотвратяване на мащабни злоупотреби с DNS:** Киберпрестъпниците често регистрират множество, понякога дори хиляди, имена на домейни за кратък период от време. Това се отнася особено за фишинг, разпространение на зловреден софтуер и съдържание, нарушаващо авторските права. Гарантирането, че търсещият законен достъп може да получи списък на всички имена на домейни, регистрирани с помощта на едни и същи данни за регистранта (обратна проверка на WHOIS), е от съществено значение, когато се подозират сложни и разпръснати незаконни дейности в такъв мащаб. Ето защо препоръчваме член 28 от Директива NIS2 да бъде транспониран така, че да позволява, че "*когато име на домейн е свързано с неправомерна или незаконна дейност и това се твърди от законно търсещо достъп лице, то регистрите на имена на ДПН и организациите, предоставящи услуги по регистрация на имена на домейни, трябва при поискване да предоставят на законно търсещото достъп лице списък на всички имена на домейни, които те администрират или са регистрирали със същите данни за регистранта".* **Юридически лица:** Данните от WHOIS на юридическите лица (най-малко име и работещ/проверен телефонен номер и работещ/проверен имейл адрес за връзка) трябва да бъдат публично достъпни съгласно член 28, параграф 4 във връзка със съображение 112 от Директивата NIS2.		
MPA	**Становище по прилагане на Директивата NIS2: постигане на целта на член 28 за публичен достъп до надеждна информация за WHOIS (част 4)** **Проверка:** Процедурите за проверка на данните от WHOIS трябва да бъдат надеждни и постоянно актуализирани, за да	**Не приема предложението.**	По смисъла на предложението на ЗИД на ЗКС, за регистрите на имена на домейни от първо ниво и субектите, предоставящи

	отразяват подобренията в технологиите и процесите. Както е посочено в съображение 111 от Директива NIS2, тези процедури следва да "предотвратяват и коригират неточни данни за регистрация" и следва да "отразяват най-добрите практики, използвани в индустрията [. . .], и напредъка, постигнат в областта на електронната идентификация" и следва да включват както "предварителни проверки, извършвани по време на регистрацията, така и последващи проверки, извършвани след регистрацията". Въпреки че регистрите на имена на ДПН може да не са в състояние да проверяват данните от WHOIS по време на регистрацията, тъй като първоначалното събиране на данните обикновено се извършва от регистраторите и/или услугите за защита на личните данни/прокси сървърите, те със сигурност могат да предприемат последващи процедури за проверка на данните от WHOIS. Препоръчваме законопроектът да направи задължителни предварителните и последващите процедури за проверка за регистрите на имена на ДПН. Освен това следва да се предвидят последици за подаването на неправилни, неточни или непълни регистрационни данни. Ние категорично подкрепяме прилагането на този подход от страна на Белгия[5] при транспонирането на член 28 от Директива NIS2, както следва: *"Ако данните за регистрация на име на домейн, изброени в параграф 1, точка 2 на име на домейн, са неправилни, неточни или непълни, регистрите на имена на домейни от първо ниво и организациите, предоставящи услуги за регистрация на имена на домейни, незабавно блокират работата на това име на домейн, докато притежателят на името на домейн не коригира данните за регистрация, така че те да станат правилни, точни и пълни*. *Ако регистрантът на име на домейн не направи това в рамките на срока, определен от регистъра на име на домейн от първо ниво или от организацията, предоставяща услуги за регистрация на имена на домейни, името на домейн се анулира*.		услуги за регистрация на такива имена на домейни, т.нар. Субекти по смисъла на чл. 27в, ал.1, са длъжни да създават и поддържат политики и процедури, включително процедури за проверка и разкриване на информация, които осигуряват спазването на следните изисквания: събират и поддържат точни и пълни данни, при спазване изискванията областта на защитата на личните данни, съхраняват информацията необходима за установяване и осъществяване на връзка с притежателите на имена на домейни, при изпълняване задължението да създават и поддържат политики и процедури, включително процедури за проверка и разкриване на надлежната информация. Дефинирането на понятието за „поддържане“ на политики, означава своевременна и надеждна актуализация.

	Трансферът на блокирано име на домейн към друга организация, предоставяща услуги по регистрация на имена на домейни, е забранен."		
MPA	**Пълен регистър WHOIS (Thick WHOIS)**: Регистърът на единни имена на ДПН за .com и .net отговаря за повече от половината от всички регистрирани имена на домейни в световен мащаб и има договори с повече от 2000 регистратори по целия свят. Понастоящем правителствените агенции и други лица, които търсят законен достъп, са принудени да открият съответния регистратор, за да поискат данни от WHOIS. Трудният процес, който това налага, както и фактът, че регистраторът може да се намира в държава, която не сътрудничи по отношение на такива искания, напълно подкопават целта за повишаване на киберсигурността и вместо това служат за прикритие и защита на незаконните участници. Поради това е от съществено значение този регистър, както и всички други регистри на имена на ДПН, да поддържат пълна, точна и независима база данни на WHOIS за **всички** имена на домейни, които администрират (наричана "дебела WHOIS"), като тези данни **трябва да включват** данните на действителния потребител на името на домейна, а не просто данните на доставчика на услуги за защита на личните данни или прокси, които може да са били използвани в процеса на регистрация (вж. по-горе). Това съществено изискване ще гарантира, че правоприлагащите органи и други лица, законно търсещи достъп, разполагат с централизиран и единен източник, от който да черпят пълни и точни данни за всяко име на домейн, администрирано от регистъра на имена на ДПН.	**Не приема предложението.**	Регистър (Thick WHOIS) за .com и .net отговарящ за регистрираните имена на домейни в световен мащаб, не е предмет на българска регулация.
„ДОМЕЙН МЕНАДА” ЕООД	1. „Домейн Менада“ ЕООД попада под определението за предприятие за производство на храни, съгласно определението в член 3, точка 2 от Регламент (ЕО) № 178/2002 на Европейския парламент и на Съвета. Проектът не изяснява по категоричен начин дали всички производители на храни се класифицират като „важни субекти“ или за някои ще са приложими правилата за „съществени субекти“. В тази връзка, намираме за необходимо, предвидения в § 5 от Проекта чл. 4а да се	**Приема се по принцип** **Приема се по принцип.**	В чл. 4. се определят изискванията към: *2. публични и частни субекти от видовете, посочени в приложение I или II,* като допълнително в методиката предвидена в чл.16, ал.1 т.8 се предвижда задължение за компетентните органи да уведомят всеки задължен субект,

	допълни, като се възложи задължение на компетентните административни органи по прилагането и изпълнението на Закона, да уведомят всеки от задължените субекти, в изрично определен в Закона срок, като какъв е класифициран - „съществен“ или „важен“, за да се избегне възможността за неправилно тълкуване от страна на самите субекти относно тяхното качество и оттук - неправилно прилагане на Закона. Считаме, че с оглед на това, че в чл. 3, параграф 5 от Директива (ЕС) 2022/2554 на Европейския парламент и На Съвета от 14 декември 2022 година относно мерки за високо общо ниво на киберсигурност в Съюза, за изменение на Регламент (ЕС) №910/2014 и Директива (ЕС) 2018/1972 и за отмяна на Директива (ЕС) 2016/1148 („Директива МИС 2“) е възложила на компетентните органи да уведомяват ЕК за броя на всички съществени и важни субекти във всеки сектор и подсектор, горното ни искане не би представлявало допълнителна тежест на компетентния орган, а би спестило каквото и да било объркване в задължените лица.		относно неговата класификация - „съществен“ или „важен“.
„ДОМЕЙН МЕНАДА” ЕООД	2. Съгласно на член 6, параграф 3 от Директива (ЕС) 2022/2557 на Европейския парламент и на Съвета от 14 декември 2022 година за устойчивостта на критичните субекти и за отмяна на Директива 2008/114/ЕО на Съвета, всяка държава членка съставя списък на установените критични субекти и гарантира, че в срок от един месец от установяването им тези критични субекти се уведомяват за това установяване. Предлагаме кореспондиращо уведомяване да намери приложение и в настоящия Проект.	**Приема се по принцип.**	В ЗИД на ЗКС съществува нарочно задължение за уведомяване на Европейската комисия, в определен срок за идентифицираните съществени и важни субекти на закона.
„ДОМЕЙН МЕНАДА” ЕООД	3. Отправяме предложение в § 4 от Проекта относно чл. 4, т. 2 и в § 5 от Проекта относно чл. 4а, ал. 1, т. 1 да бъде направено уточнение дали приложението на Закона по отношение на предприятия, които отговарят на критериите за средни предприятия съгласно чл. 3, ал. 1 от Закона за малките и средни предприятия, или надхвърлят таваните за	**Не приема предложението.**	Препратката към ЗМСП, а именно „Чл. 3. *(Изм. - ДВ, бр. 59 от 2006 г.) (1) Категорията малки и средни предприятия включва предприятията, които имат:*

	средни предприятия от посочения член, се отнася само до независими предприятия или в това число биват разглеждани и предприятия-партньори и свързани предприятия по смисъла на ЗМСП. **Пояснение:** Въпросът възниква в хипотезата на българско дружество, което само по себе си не отговаря на критериите за средно предприятие, но в случай, че бъде разглеждано заедно със свързаните му предприятия извън България, то би отговаряло на тези критерии.		*1. средносписъчен брой на персонала, по-малък от 250 души, и* *2. годишен оборот, който не превишава 97 500 000 лв., и/или стойност на активите, която не превишава 84 000 000 лв.* *(2) От предприятията по ал. 1 малки предприятия са тези, които имат:* *1. средносписъчен брой на персонала, по-малък от 50 души, и* *2. годишен оборот, който не превишава 19 500 000 лв., и/или стойност на активите, която не превишава 19 500 000 лв.* *(3) От предприятията по ал. 1 микропредприятия са тези, които имат:* *1. средносписъчен брой на персонала, по-малък от 10 души, и* *2. годишен оборот, който не превишава 3 900 000 лв., и/или стойност на активите, която не превишава 3 900 000 лв.“*, се тълкува във връзка с чл.4, който дефинира *„…изчисляване на данните по чл. 3 се взема предвид дали предприятието е независимо, дали е предприятие партньор по смисъла на ал. 3, или е свързано предприятие по смисъла на ал. 5.“* В допълнение ще бъде издадена Методика за определяне на съществените и важни субекти за целите на ЗКС.
„ДОМЕЙН МЕНАДА” ЕООД	4.Във връзка със задължението на субектите по изменените чл. 3, ал. 4 и чл. 22 от Закона да приемат и прилагат различни политики, правила и процедури, моля да предвидите	**Приема се по принцип.**	в процедурата по изменение и допълнение на НМИМИС ще се предвиди

	изготвянето на образци на примерни правила и политики с минимално задължително съдържание за субектите, които се квалифицират като „важни“. Препоръката е с оглед спецификата на материята в Закона, по която не всеки задължен субект разполага с вътрешни ресурси с такива специални и технически знания и компетенции. Голяма част от субектите за първи път ще бъдат задължени лица по Закона, поради което и привеждането на дейността им в съответствие представлява голяма финансова и административна тежест, която би могла да бъде смекчена от възможността да се използва стандартизиран вариант на правила и политики. Образците биха били от полза и да се постигне сравнително унифициран подход от страна на задължените субекти. Допълнително, такъв подход беше предприет от ДАНС във връзка с Закона за мерките за изпиране на пари и приемането на вътрешни правила по него.		обсъждането на такова предложение относно стандартизиран вариант на правила и политики.
„ДОМЕЙН МЕНАДА” ЕООД	5. Намираме за необходимо в § 24 от Проекта относно чл. 23 да се предвиди срок, в който да бъде изготвена координирана оценка на риска за сигурността на критични вериги за доставки. Ясното поставяне на краен срок е необходимо за задължените субекти, с оглед значимостта и обвързаността на оценката на риска по променения чл. 23 от Закона при определяне на подходящи мерки по смисъла на променения чл. 22, ал. 3 от Закона.	**Приема предложението.**	
„ДОМЕЙН МЕНАДА” ЕООД	6. Считаме, че редакцията на чл. 27к, ал. 1 и ал. 2 от Закона следва да бъде съобразена с текста на член 32, параграф 5 от Директива МИС 2, като се предостави допълнителен срок, който да бъде дефиниран, за субектите да предприемат необходимото действие в съответствие с изискванията на	**Не приема предложението.**	Директивата не предвижда такъв отлагателен срок, разпоредбите приети в изпълнение на задължението за

	тези органи. Новите принудителни мерки по чл. 27к, ал. 1 и ал. 2 от Закона следва да бъдат прилагани едва след като изисканото действие не бъде предприето в определения срок. Допълването в чл. 27к ще предостави на задължените субекти още една възможност за поправка на поведението им, която е предвидена в Директива МИС 2, преди налагането на предвидените санкционни действия, които сами по себе си са достатъчно сериозни, за да бъдат директно приложени.		транспониране следва да започнат да се изпълняват от 18 октомври 2024 г.
„ДОМЕЙН МЕНАДА” ЕООД	7. Моля, изречението „За тези лица се прилагат всички мерки предвидени както за съществените, така и за важните субекти“ от чл. 27к, ал. 5 да отпадне, тъй като е неясно и не кореспондира на текст в Директива МИС 2.	**Не приема предложението.**	Законодателя предлага редица мерки както за съществените, така и за важните субекти в чл.27ж, съответно ал.1 за съществените и ал.2 за важните, както и мерките в Чл. 27и, които предхождат мерките по чл.27к. Надграждането от предупреждение, през одит до администинстративно наказание е ясно дефинирано в горепосочените членове. Кореспондира с чл.33, т.5 от Директивата т. 5 - Член 32, параграфи 6, 7 и 8 се прилагат *mutatis mutandis* за надзорните и правоприлагащи мерки, предвидени в настоящия член за важните субекти.

„ДОМЕЙН МЕНАДА” ЕООД	8. Член 36 от Директива МИС 2 предвижда санкциите, установени от държавите-членки от да бъдат ефективни, пропорционални и възпиращи. Намираме, че заложените в Проекта санкции не са пропорционални, а напротив - санкциите са в прекалено високи размери и макар да кореспондират със санкциите съгласно Директива МИС 2, то същите са прекомерни с оглед българския стандарт на живот и икономическата ситуация в страната, и биха могли да доведат до изпадане в несъстоятелност и фалит на редица задължени субекти, което от своя страна би имало негативно влияние върху нормалното функциониране на пазара. Считаме, че максималните прагове следва да бъдат запазени съгласно размера в Директива МИС 2, а не да бъдат увеличени. Считаме, че минимално установените санкции също следва да бъдат намалени, още повече че за тях няма конкретно изискване в Директива - МИС 2 и санкция от 100 000 лв. или 200 000 лв. ще е непосилна за субектите, особено за тези, които не са ангажирани пряко с предоставяне на онлайн услуги, ИТ услуги, кредитни институции и др. под. Санкции в по-ниски размери също биха отговорили на критериите да са ефективни, пропорционални и възпиращи, без да са свръхнатоварващи и да излизат от посочените функции в негативен аспект.	**Приема се.**	
„ДОМЕЙН МЕНАДА” ЕООД	9.Намираме, че предвидената в чл. 29, ал. 6 от Закона санкция за управителите следва да отпадне изцяло, като се вземе предвид санкцията по чл. 27к, ал. 5, която сама по себе си е достатъчно сериозна. Кумулирането на двете санкции би било непропорционално, а и конкретна глоба за управителните органи не е предвидена в Директива МИС 2,	**Приема се по принцип.**	За управителите или членовете на управителните органи на съществените и важните субекти е предвидена санкция в случай че не изпълнят

	с оглед на което не е задължително българският нормотворец да приема по-утежняващи условия за българските задължени субекти.		задълженията си по чл. 21 от ЗИД на ЗКС.
„ДОМЕЙН МЕНАДА” ЕООД	10.Периодичните и имуществени санкции в чл. 30а са в прекомерен размер и намираме, че следва да бъдат намалени или да отпаднат, предвид, че се налагат за всеки ден неизпълнение, а Директива МИС 2 само предвижда възможност за приемане на такива мерки без да създава конкретно задължение за държавите членки,	**Приема се.**	
„ДОМЕЙН МЕНАДА” ЕООД	11. От текста на Проекта не става ясно какъв е срокът, в който субектите следва да имплементират мерките и от кой момент са задължени да започнат да ги прилагат. Предлагаме, в Преходните и заключителните разпоредби на Проекта да бъде заложен изричен срок (който може да е определени месеци след приемането на наредбата по § 40, т. 2 от Проекта, приемането на оценката по § 24 от Проекта относно чл. 23 от Закона и получаването на съобщение какъв задължен субект е съответното лице), за да може задължените субекти да имат време за планиране на необходимите ресурси, за подготовка и имплементиране на необходимите правила и политики.	**Не се приема.**	Директивата не предвижда такъв отлагателен срок. Законовите разпоредби влизат в сила от датата на влизане в сила на закона. Съгласно Директивата, разпоредбите приети в изпълнение на задължението за транспониране следва да започнат да се изпълняват от 18 октомври 2024 г.
b.bozhanov	**Премахване на текстове от Закона за защита на класифицираната информация** Предлагам въвеждане на нов параграф в преходните и заключителни разпоредби, с който да бъде изменен Закона за защита на класифицирана информация, по отношение на Приложение 1, част II, като предлагам т. 14 да бъде отменена.	**Не приема предложението.**	В ПЗР на ЗИД на ЗКС не е релевантно, без обсъждане и координиране на процеса по изменението с отговорните органи в конкретната сфера а именно Държавна комисия по сигурността на информацията (ДКСИ) да се правят изменения, които са в тяхната компетентност.

	За постигане на високо ниво на киберсигурност, добрите практики изискват адекватна документация на процесите и практиките, конфигурациите, автоматизиране на дейностите. В допълнение, закупуването на решения (хардуерни и софтуерни) за киберсигурност следва да бъде максимално прозрачно и конкурентно. Предложената за отмяна т. 14 съдържа пречки за ефективното изпълнение на дейности, свързани с киберсигурността, поради особения режим на работа с класифицирана информация. Сигурността на информационните системи се базира не на прикриването на информация, а на нейната навременна достъпност за експертните лица, поради което нейното класифициране следва да отпадне. Алтернативно, може да бъде стеснен обхвата на информацията по т. 14, конкретно до информация за защита на криптографски ключове.		
strategy_bg-NS	**Относно периодичните санкции и предвидената методика по чл. 16, ал. 3, т. 8** 1. Предлагам да се измени или изцяло премахне §31, с който се създава чл. 30а. Директивата представя единствено възможност за периодични санкции, поради което същата или трябва да се премахне изцяло, или следва да се	**Приема се.**	

	намали значително размера ѝ, тъй като предвиденият в ЗИД размер от 5000 лв. на ден е прекомерен. Ако периодична санкция остане, то същата следва да се намали значително или да се предвиди, че е най-малко за всеки месец. В нито един закон не се предвижда подобна огромна санкция, а ако такава санкция бъде наложена на практика - то тя би могла да доведе до несъстоятелност на почти всяко едно дружество в страната. 2. Предлагам в закона или методиката, която ще се приеме съгласно §31, да се предвиди изрично възможността, описана в преамбюл 16 от Директивата МИС 2. 3. В §40 следва да се направи промяна като референцията към чл. 4, ал. 3 се промени на чл. 16, ал. 3, т. 8	**Приема се по принцип.** **Приема се.**	Съгласно чл. 16, ал. 3, т. 8 следва да бъде приета Методика за определяне на съществените и важни субекти за целите на ЗКС.
Фондация „Право и Интернет“	**1.1.** Относно §3 ЗИД, който предвижда изменение на чл. 3, ал. 2 ЗК. ➢ При анализ на текста става ясно, че е налице техническа грешка в препратката, която следва да бъде към „*чл. 4, т. 3, буква „а*“ (т.е. следва да отпадне текстът *ал. 1*). ➢ Прави впечатление и обстоятелството, че към настоящия момент се получава празнота относно приложимите за лицата по чл. 4, т. 3, буква „а“ мерки. Към настоящия момент за „доставчици на обществени електронни съобщителни мрежи или на обществено достъпни електронни съобщителни	**Приема се.** **Приема се.**	

	услуги“ се прилагат Правилата за минималните изисквания за сигурност на обществените електронни съобщителни мрежи и услуги и методи за управление на риска за тяхната сигурност на Комисията за регулиране на съобщенията (Правилата), приети съгласно чл. 243б от Закона за електронните съобщения (ЗЕС). Затова би следвало да се предвиди изрична разпоредба, сходна на тази по чл. 3, ал. 2, която предвижда какъв нормативен акт ще се приеме за тези субекти и кой орган ще го приема (от новия чл. 24, ал. 1 изглежда, че в процеса на изготвяне на ЗИД е имало нещо в този смисъл, но по технически причини явно е отпаднало). ЗИД не указва и дали Правилата се отменят изрично или ще продължат да се прилагат след приемането на ЗИД. удазно е това да се направи – напр. чрез изрична допълнителна точка в този смисъл в §42 от ЗИД, който към момента урежда, че Комисия за регулиране на съобщенията (КРС) ще е националният компетентен орган по ЗК за тези субекти. Това е особено важно с оглед изричната отмяна на Глава петнадесета, раздел I от ЗЕС, в която именно се съдържа основанието за приемане на Правилата (§42, т. 3 ЗИД). Поради това е препоръчително да се предвиди изрично дали и докога Правилата ще продължат да се прилагат, и дали ще се приемат от КРС или от друг орган. В контекста на действащите към момента Правила, например, би могло да се укаже, че Правилата ще останат в сила до приемането на нов подзаконов нормативен акт, който урежда конкретните мерки за лицата по чл. 4, т. 3, буква „а“. Основните разпоредби на Правилата са в сила от малко повече от една година и са съобразени в голяма степен с действащата нормативна уредба и		

	специфичните потребности на този сектор. А доколкото КРС се предвижда да бъде национален компетентен орган за тези субекти и е такъв и досега, то логично би било КРС самостоятелно или, например, съвместно с Министерството на електронното управление да приеме тези актове. Горното е особено важно и в контекста на новите чл. 5, т. 3 и чл. 6а (§8 ЗИД), доколкото част от субектите вероятно попадат и там. Съответно няма яснота относно съотношението между правните норми. Наличието на отделни правила за тези субекти е оправдано и с оглед преамбюл 95 от Директивата. ➢ С цел олекотяване на текста, за да се избегне конструкцията „*с изключение на посочените в чл. 4, ал. 1, т. 3, буква „а“,* може да се предложи изменение в ал. 3, което да гласи: „*(3) Наредбата по ал. 2 не се прилага за ведомствата и функциите им по чл. 5, т. 2, както и за субектите по чл. 4, ал. 1, т. 3, буква „а“.*“ Това разбира се е под условие и изцяло в зависимост от подхода относно Правилата.	**Приема се по принцип.**	
Фондация „Право и Интернет“	**1.2.** За постигане на по-добър баланс при въвеждане на Директивата считаме, че могат да се обсъдят и предложат някои промени в предложения обхват на ЗК, за да се постигне по-голяма яснота и прецизност ➢ Относно чл. 4, т. 1 – „административни органи“ (§4 ЗИД) След внимателен анализ на предложените изменения от гледна точка на обхвата на закона бихме искали да обърнем внимание, че	**Приема се.**	относно мерки за високо общо ниво на сигурност на мрежите и информационните системи в Съюза (ОВ, L 194/1 от 19 юли 2016 г.) в ДР § 3. „По смисъла на този закон:

	дефиницията на административни органи, която досега бе чрез препращане към §1, т. 1 от Допълнителните разпоредби на Закона електронното управление (ЗЕУ), която пък препраща към §1, т. 1 от Административнопроцесуалния кодекс (АПК) (сега с §33, т. 3 ЗИД се предлага директна препратка към АПК), може да доведе до изключително разширително тълкуване, което да включи в обхвата огромен брой субекти, които не са предвидени изобщо в Директивата. Това се дължи на следното. Съгласно §1, т. 1 АПК „*Административен орган“ е органът, който принадлежи към системата на изпълнителната власт, както и всеки носител на административни правомощия, овластен въз основа на закон включително лицата, осъществяващи публични функции, и организациите, предоставящи обществени услуги*. От това е видно, че в обхвата на административни органи влизат изцяло: *а) лицата, осъществяващи публични функции,* *б) организациите, предоставящи обществени услуги, и* *в) всеки друг всеки носител на административни правомощия, овластен въз основа на закон*. Съгласно §1 от Допълнителните разпоредби на ЗЕУ пък дефинициите по т. а) и б) са следните: *11. „**Лица, осъществяващи публични функции**“ са нотариусите, частните съдебни изпълнители, държавните и общинските учебни заведения, държавните и общинските лечебни заведения възложителите по чл. 5, ал. 2 - 4 от Закона за обществените поръчки, които не са административни органи или организации, предоставящи обществени услуги, и други лица и*		административна услуга е констатации „разшифроват” предмета на ЗЕУ в обсъжданата му част като уреждане на административното производство за издаване на определени видове административни актове по електронен път. Анализът на предмета в частта „предоставянето на административни услуги по електронен път” продължава със съпоставянето на още две разпоредби – § 1, т. 3 и чл. 39. Според дефиницията на § 1, т. 3 „вътрешна административна услуга” притежава качествата: първо, на вид административна услуга – и като такава попада в предмета на закона; второ, услугата се предоставя от един орган на друг за осъществяване на неговите правомощия. Съпоставката на тази дефиниция с чл. 39 от закона води до заключението, че вътрешните електронни административни услуги са административни производства, в които участва повече от един

	организации, чрез които държавата упражнява своите функции и на които това е възложено със закон. *14. „**Организация, предоставяща обществени услуги**“ е всяка организация независимо от правната форма на учредяването ѝ, която предоставя една или повече услуги по т. 12.* *12. „**Обществени услуги**“ са образователни, здравни, водоснабдителни, канализационни, топлоснабдителни, електроснабдителни, газоснабдителни, телекомуникационни, пощенски, банкови, финансови в т. ч. застрахователни и удостоверителни по смисъла на Регламент (ЕС) № 910/2014 или други подобни услуги, предоставени за задоволяване на обществени потребности, включително като търговска дейност, по повод на чието предоставяне могат да се извършват административни услуги.* Горното показва, че ако се запази дефиницията на административен орган с препращане към АПК/ЗЕУ, в обхвата на закона на практика ще попаднат неограничен брой субекти от всички възможни сектори, което няма да съответства изцяло на преследваните с Директивата цели и ще създаде огромни затруднения на практика (както за субектите, така и за правоприлагащите и правораздаващите органи). Това е така, защото в обхвата на организациите, предоставящи обществени услуги, се вижда, че немалка част от обществените услуги по §1, т. 12 от ДР на ЗЕУ се припокриват с услугите от секторите по новите приложения I и II. В допълнение, обхвата на тази дефиниция значително надхвърля секторите по новите приложения I и II, като практически включва всеки възможен сектор в страната.		административен орган и се осъществяват чрез използването на електронни средства. Разширеният предмет. С чл. 40, ал. 1 предметът на закона включва също междуорганизационните административни производства, свързани с осъществяване на правомощията на административните органи. Съществено, което трябва да се подчертае тук е, че посредством тази разпоредба предметът на закона включва не само производствата по предоставяне на административни услуги, но и всички производства, „свързани с осъществяване на правомощията им”. Задължението е общо и обхваща услуги, „свързани с осъществяване на правомощията им”, т.е. с масата на всичките им правомощия като административни органина действащия закон е тази за „Обществените услуги“ съгласно §1, т. 11 вр. с 12 от ДР на ЗЕУ, доколкото една от обществените услуги е

	Същото важи и за дефиницията на лицата, осъществяващи публични функции, която видно от дефиницията по §1, т. 12 от ДР на ЗЕУ, включва кръг субекти, които изобщо не са предвидени в Директивата, не са и органи на публичната администрация по смисъла на приложение I, сектор 10, член 2, параграф 2, буква е) от Директивата или чл. 2, параграф 5, буква а) от Директивата. Допълнителен проблем би могъл да изникне на практика и в контекста на определянето на съответните лица като съществени, респективно важни, защото съгласно предложеният с §5 от ЗИД чл. 4а, ал. 1, т. 4 съществени субекти ще са всички лица по т. 4, т. 1 ЗК, независимо от размера и сектора на предприятията. Така в България на практика може да се окаже, че в обхвата на новите разпоредби попадат абсолютно всички компании и сектори, и то всички ще бъдат съществени субекти. Считаме, че това е препоръчително да се коригира, за да се избегнат практически проблеми. **По-конкретно предложение в тази насока е да се въведе самостоятелна дефиниция в ЗК на административен орган, която да не допуска коментираното дублиране и повторение на сектори, например:** ***„Административен орган“ е органът, който принадлежи към системата на изпълнителната власт.*** Така се запазва изискването и съответствието с член 2, параграф 2, буква е) и параграф 5 от Директивата. Вариант, който може да се обсъди е, и да се препрати изрично към разпоредбите от Закона за администрацията, указващи органите на		именно образование, а едни научноизследователски дейности от критично значение. Секторните националните компетентни органи при определянето на субектите по реда на чл. 16, ал. 3, т. 8, ще имат за цел да идентифицират горецитираните организации по определена от самите тях принадлежност и по размер, спрямо метод **1, буква е), точка i) от Директивата, и уточняване кои от тях ще са съществени и кои важни (с оглед чл. 3, параграф 1, буква г) от Директивата**

	изпълнителната власт, за да има пределна яснота кои са субектите в обхвата. ➢ На следващо място, ако дефиницията на административни органи остане в този си вид, ще се създаде конфликт и сериозни затруднения при тълкуването на това кои образователни институции ще бъдат задължени субекти по закона – тези по новопредложения чл. 4, т. 6 (т.е. опцията по чл. 2, параграф 5, буква б) от Директивата) или тези съгласно §1, т. 11 вр. с 12 от ДР на ЗЕУ, доколкото една от обществените услуги е именно образование, а едни от лицата с публични функции по §1, т. 11 от ДР на ЗЕУ са държавните и общинските учебни заведения. Това противоречие създава формални предпоставки за тълкуване в посока, че всички образователни институции следва да попадат в обхвата (бидейки обществени услуги и едновременно част от дефиницията на лицата, осъществяващи публични функции) – без значение дали извършват научноизследователски дейности от критично значение или не, тъй като по-тясната формулировка на новата разпоредба ще се погълне от по-широката в чл. 4, т. 1. Съответно, ако не се извършат изменения в посока да се ограничи дефиницията на чл. 4, т. 1, то на практика ще има сериозни затруднения за субектите и за националните компетентни органи при определянето на субектите по реда на чл. 16, ал. 3, т. 8, предложен със ЗИД. Доколкото ЗИД очевидно цели да се възползва от опцията по чл. 2, параграф 5, буква б) от Директивата, която има далеч по-ограничен обхват, а именно да се регулират само образователните институции, когато извършват научноизследователски дейности от критично		

	значение, то е препоръчително да се направи ревизия, с която да се избегне подобно противоречие и да се поясни, че само тези образователни институции са в обхвата на закона. В този контекст е препоръчително да се помисли и за въвеждане на дефиниция на образователни институции и научноизследователска дейност, тъй като такива в момента липсват (като за второто може да се ползва дефиницията на чл. 6, т. 41 от Директивата във връзка с преамбюл 36 от Директивата). ➢ От гледна точка на чл. 2, параграф 5, буква а) от Директивата може да се помисли и дали от обхвата на дефиницията на административни органи да не отпаднат органите на публичната администрация на местно равнище (това вероятно следва да са териториалните органи на изпълнителната власт – кметове ведно с администрациите им, областни управител и администрации, както и други специализирани териториални администрации), като се вземе предвид внимателно и чл. 6, т. 35 от Директивата. Аргументите отново са в посока, че се разширява значително обхватът на закона за лица, които са предвидени единствено като опция в Директивата, която от своя страна цели унифициран подход за ЕС и консистентност в държавите-членки. В допълнение, привеждането в съответствие с тези нови правила за тях би изисквала изключително сериозен финансов и административен капацитет, който редица по-малки администрации не биха могли да осигурят. Съответно, с цел консистентност на европейско ниво може да се обсъди такъв подход, макар че	**Не се приема.**	

	същевременно ясно отчитаме необходимостта и критичния характер на дейността на тези органи, което е и причината те да са част от обхвата. Поради това, ако все пак не може да се възприеме такова предложение, може да се обсъди по-облекчен ред и режим за тях. ➢ В пряка връзка с изложеното дотук относно дефиницията на административни органи, на принципно ниво изглежда обосновано предложените т. 7 и 8 на чл. 4 да отпаднат изцяло (ведно със съответната редакция на дефиницията на административни органи). Причините са сходни на изложените нагоре. Тези две т. 7 и 8 в исторически план са имали за цел да включат лица от този кръг субекти само в един конкретен случай – когато предоставят административни услуги по електронен път (и защото не са били регулирани на друго основание). С разширяването на обхвата съгласно Директивата, респективно на нашия закон, на този етап изглежда ненужно кръгът субекти по т. 7 и 8 да остане, тъй като така или иначе обхватът на закона е значително разширен и се дублира на не малко места. Освен това се получава припокриване с другите основания: а) със секторите в приложения I и II; и б) дефиницията на административни органи, която така или иначе включва в себе си организациите, предоставящи обществени услуги и лицата, осъществяващи публични функции, но без ограничението по чл. 4, т. 7 и 8, че се отнася до случаите, в които предоставят административни услуги по електронен път. ➢ Не на последно място следва да се отбележи, че допълнителни затруднения ще възникнат на практика и по отношение на онези субекти, при които има припокриване между основното правно		

	основание и дефиницията на административни органи. Например: субектите от сектор „Пощенски услуги“ формално могат да попаднат в обхвата както на основание новите чл. 4, т. 2 (с оглед Приложение II, сектор 1), така и на основание §1, т. 12 от ДР на ЗЕУ, тъй като едни от обществените услуги са именно пощенските услуги. Сходно е положението за телекомуникационните, удостоверителните, електроснабдителните и т.н. услуги. Това създава конфликт между нормите, поради което спорен ще остане въпросът кой ще е националният компетентен орган и на кое основание за тези сектори, тъй като за субектите – административни органи национален компетентен орган по чл. 16 ЗК е Министерство на електронното управление. За всеки сектори пък национален компетентен орган по чл. 16 ЗК е съвсем различен орган, поради което е препоръчително да се направят съответните редакции в текста. Конкретно за пощенските услуги е препоръчително да се обърне внимание и на преамбюл 12 от Директивата, съгласно който определени дейности на доставчиците на пощенски услуги не следва да попадат в обхвата на регулацията. По сходен начин преамбюл 11 от Директивата посочва и, че за някои специфични удостоверителни услуги (по смисъла на Регламент (ЕС) № 910/2014) изискванията на Директивата не следва да се прилагат. ➢ В контекста на изложеното относно административните органи следва да се отбележи и, че е налице разминаване между предложеният чл. 4а, ал. 1, т. 4 ЗК и чл. 3, параграф 1, буква г) от Директивата, защото Директивата изисква съществени субекти да са само лицата по чл. 2,		

	параграф 1, буква е), точка i) от Директивата, а не всички органи на публичната администрация. Това предпоставя известно несъответствие с Директивата, поради което е препоръчително да се ревизира като се уточни кои са съществени и кои важни субекти. ➢ **В обобщение на изложеното по тази точка:** Ако се запазят текстовете от ЗИД по предложения начин, има риск да се създадат формални условия за прекомерно разширяване на обхвата в сравнение с NIS 2, което да доведе до затруднения от практическо естество както за националните компетентни органи, така и за субектите и търговията като цяло. Внасянето на редакции изглежда обосновано и в контекста на преследвания от държавата балансиран подход по транспониране (максимален баланс между заложените в Директивата цели/обхват и местното законодателство) и с оглед постигането на по-високо ниво на хармонизация на ниво ЕС. Освен това, от гледна точка на националните компетентни органи, например, разширеният обхват на субектите би довел до сериозни затруднения при упражняване на правомощията им както в контекста на засиленото международно сътрудничество, така и с оглед новите надзорни и контролни правомощия, които се въвеждат. Не на последно място, ограничаването на обхвата на ЗК в максимална степен до обхвата на Директивата би било обосновано и в контекста на това, че редица компании – вкл. средни и големи предприятия по смисъла на Препоръка 2003/361/ЕО, трудно могат да си позволят бюджета и административния		Териториалните органи на изпълнителната власт – кметове ведно с администрациите им, областни управител и администрации, както и други специализирани териториални администрации са субект и на сега действащия Закон за киберсигурност и изключването им би било крачка назад по отношение на постигането на високо общо ниво на мрежова и информационна сигурност на национално ниво.

	капацитет, необходим за спазване на новите правила. Добре известно е, че от гледна точка на специалисти в сферата на киберсигурност е налице голям дефицит, който не би могъл да се реши в рамките на месеци. Съответно, ако всички субекти трябва да се назначат служители по сигурността, то това допълнително би затруднило субектите. Този проблем би се задълбочил, ако в обхвата на закона попадат лица, за които това по принцип не се предвижда и които не пораждат съществени рискове. Предвид горното изглежда препоръчително да се извърши допълнителен анализ и да се отстранят споменатите потенциални затруднения за тълкуване и прилагане на практика, и да се постигне по-балансирано въвеждане на новите правила, вкл. за да се избегнат рисковете от неправилно транспониране на Директивата и ненужно разширяване на обхвата му. **В заключение, предложението ни е за:** - въвеждане на самостоятелна дефиниция на понятието административни органи, която да се стесни с оглед съображенията ни нагоре (само така ще има пределна яснота кои субекти попадат в обхвата, което ще подпомогне значително националните компетентни органи при действията им по определянето на субектите по реда на новия чл. 16, ал. 3, т. 8 от ЗИД). - отпадане изцяло на т. 7 и 8 на чл. 4 ЗК, - уточняване на обхвата на образователните институции, както и		

	- евентуално стесняване на обхвата на самите административни органи до тези по член 2, параграф 1, буква е), точка i) от Директивата, и уточняване кои от тях ще са съществени и кои важни (с оглед чл. 3, параграф 1, буква г) от Директивата. – Такъв подход би съответствал и на заложените цели в преамбюли 4 до 8 от Директивата за уеднаквяване на изискванията в държавите членки, особено с оглед субектите, предлагащи трансгранично стоки и услуги. Освен това, ако няма пределна яснота кой субект на кое основание и за коя услуга е определен като субект, то страната ни може да срещне трудности при изпълнение на задължението си по чл. 3, параграф 5, буква б).		

Фондация „Право и Интернет“	1.3. Относно §3, т. 4 ЗИД - Предложеният текст на чл. 3, ал. 4 е препоръчително да се изтрие, тъй като не става пределно ясно дали и каква функция има (напр. дали това са задължения за субектите, предметна рамка на закона или нещо друго) в контекста на предложения в §24 ЗИД – чл. 22, който транспонира чл. 21 от Директивата. При преглед на текста на ЗИД изглежда, че е налице дублиране с повечето точки от предложения чл. 22, ал. 2, поради което може би чл. 3, ал. 4 следва да отпадне изцяло.	**Приема се.**	
Фондация „Право и Интернет“	1.4. Относно чл. 4, т. 1 (§4 ЗИД) Предложеният текст на чл. 4, т. 1 реферира към чл. 3, ал. 1 от Закона за малките и средни предприятия. В същото време Директивата реферира към критериите по член 2 от приложението към Препоръка 2003/361/ЕО. За да се избегне разминаване и с оглед постигане на по-добра хармонизация, бихме препоръчали да се направи допълнителен анализ дали двете дефиниции се припокриват.	**Приема с епо принцип.**	
Фондация „Право и Интернет“	**1.5.** В §5 ЗИД се предвижда създаването на чл. 4а ЗК. В текста се вижда, че е налице техническа грешка в препратките към чл. 4, като навсякъде би следвало да отпадне посочването на ал. 1.	**Приема се.**	
Фондация „Право и Интернет“	**1.6.** Относно предложения с §5 ЗИД чл. 4а, ал. 1, т. 7, който ползва опцията по чл. 3, параграф 1, буква ж) от Директивата – бихме отбелязали, че е спорно	**Не се приема.**	След направен анализ е констатирана непълнота, която трябва да бъде избегната, поради което се

	дали и доколко от този текст има смисъл, тъй като тези субекти вече попадат в някоя от категориите по чл. 4 и по-голямата част от тях ще са съществени субекти на друго основание.		запазват субектите в Чл.4а, ал. 1, т.7. определените като оператори на съществени услуги към датата на влизане в сила на настоящия закон;
Фондация „Право и Интернет“	**1.7.** Като се има предвид чл. 2, параграф 7 от Директивата бихме препоръчали да се направи допълнителен анализ, съответно редакция (ако е необходима), дали чл. 5, т. 2 и 3 (§6 ЗИД) са в пълно съответствие с посочения текст от Директивата. В противен случай има риск органи от специалните сектори да влязат в обхвата на закона, въпреки изричния текст на Директивата.	**Приема се по принцип.**	
Фондация „Право и Интернет“	**1.8.** Предложение, което заслужава внимание е и да се извърши частична промяна в статута на предвидения в чл. 6, ал. 5 ЗК регистър (§7 ЗИД). С цел осигуряване на публичност и прозрачност може да се предвиди, че регистърът има и публична версия (поне да има яснота кои са субектите), за да има максимална прозрачност за обществото.	**Не се приема.**	В регистъра е предвидено да се съдържание чувствителна информация, включително лични данни, което не обуславя наличие на публична част на регистъра по чл.6.
Фондация „Право и Интернет“	1.9. Относно §8 ЗИД Във връзка с §8 ЗИД, който въвежда чл. 6а, с оглед прозрачност и по-малко тежест за субектите, препоръчително е да се предвиди задължение за МЕУ или административните органи, съгласно което да се изготвя списък на специалните закони по чл. 6а в координация със съответните органи. По	**Не се приема.**	Компетентните органи определят кои са техните субекти и са задължени да изключат онези от тях, които подлежат на специална регулация.

	този начин както субектите, така и органите, ще имат яснота за това кои правила следва да спазват, респективно контролират. В допълнение, това ще помогне значително и за намаляване на административната тежес за органите и субектите, защото няма да се налага двукратно или дори трикратно в някои случаи уведомяване, когато има сходни по ефекта си уведомителни режими за уведомяване за инциденти. Така например в преамбюл 28 от Директивата ясно е посочено, че Регламент (ЕС) 2022/2554 е специален, поради което финансовите субекти по смисъла на този регламент няма да бъдат субекти на Закона за киберсигурност. За да може да се случи това обаче е необходимо да се прецени внимателно кои са тези субекти в контекста на сектори 3 и 4 по приложение I от Директивата и ЗИД, съответно това да се разясни на ранен етап на всички засегнати. Сходно и преамбюл 29 от Директивата дава предписания относно по-строгите актове в областта на въздухоплаването. Този проблем може да се задълбочи на практика и в контекста на чл. 5, който изключва от режима на ЗК само частично определени субекти и части от дейността/системите на субекти, които остават по принцип в обхвата на закона. В този смисъл, няма яснота дали режима по Наредбата за условията и реда за определяне на мерките за защита на информационните и комуникационните системи на стратегическите обекти от значение за националната сигурност и за осъществяването на контрол е специален спрямо ЗК. Затова е препоръчително и прецизиране в тази част.		
Фондация „Право и Интернет“		**Приема се по принцип.**	Общата уредба за административните актове и

	1.10. Относно §17 ЗИД, който предвижда нов чл. 16, ал. 3, т. 8 бихме препоръчали (с оглед гарантиране на правото на защита и основните принципи на законност и справедливост) да се предвиди изрично, че актовете на органите са административни актове, които подлежат на обжалване от субектите, определени като такива.		техните характеристики е предвидена в АПК, който урежда и реда за тяхното издаване и обжалване.
Фондация „Право и Интернет“	1.11. По отношение на §24 ЗИД ➢ Предложеният чл. 22, ал. 1, изречение второ, гласи следното: „… При спазване на принципа за технологична неутралност, съответните европейски и международни стандарти и технически спецификации, се гарантира ниво на сигурност на мрежовите и информационните системи, съответстващо на риска…“ Този текст цели да транспонира чл. 21, параграф 1, изречение второ от Директивата: „Като се вземат предвид последните постижения в тази област и, когато е приложимо, съответните европейски и международни стандарти, както и разходите за прилагането им, мерките, посочени в първа алинея, гарантират ниво на сигурност на	**Приема се.**	

	мрежовите и информационните системи, съответстващо на породените рискове.“ Съпоставка между двата текста показва голямо сходство, но и различие, което може да има съществен практически ефект при изпълнение на закона, респективно при надзора и контрола от органите. Видно от български текст, в ЗК не се предвижда да се отчитат „разходите за прилагането“ на мерките, както и да „се вземат предвид последните постижения в тази област“. В контекста на сериозните задължения, които ще бъдат наложени на субектите, считаме за необходимо законът изрично да предвиди, че при въвеждането на мерките разходите са важен критерий. Именно този текст осигурява баланс между необходимостта да се въвеждат най-новите и ефективни мерки съобразно идентифицираните рискове, но и същевременно с това мерките да са икономически обосновани от реалните възможности на субектите. Затова бихме препоръчали чл. 22, ал. 1, изречение второ да се допълни като се съобразят текстовете на Директивата. ➢Относно предложения чл. 23 в §24 ЗИД	**Приема се.**	

	Относно текста на чл. 23 бихме препоръчали да се поясни изрично, че съгласуването се прави с **националните компетентни органи по чл. 16 от закона, както и със засегнатите субекти по закон**. Сегашният текст посочва, че: „… изготвя съгласувано с компетентните органи“, но не става ясно кои са те. В допълнение, за по-голяма прецизност е препоръчителна редакция в текста, като се заимства от текста на чл. 22 от Директивата, а именно: да се замени текста „**технологичните и нетехнологичните рискове“ с „техническите и, само когато е уместно и обосновано – нетехническите рискови фактори**“. Така разпоредбата ще е в по-голямо съответствие с Директивата. Бихме препоръчали да се посочи и изрично, че **всяко ограничаване е само временно, тъй като в противен случай могат да се засегнат необосновано дълго** правата на субектите и на третите лица, част от търговския оборот. Бихме препоръчали нормата да се разгледа и обсъди допълнително с всички възможни лица, които могат да бъдат засегнати от нея. Субектите на закона са значително разширени, поради което подобни ограничения (ако бъдат въведени) могат да засегнат хиляди лица в страната – търговци на едро и дребно,	**Приема се.**	

	физически лица и т.н. Всяко подобно ограничаване на права и свободи следва да бъде пропорционално на преследваните цели, справедливо и прозрачно, и недискриминационно. В този контекст следва да се направи така, че разпоредбата да не създава възможности за неравноправно третиране на участници от едни и същи сектори, да не създава практически трудности, ако бъдат наложени такива ограничения. – коригиран текст		
Фондация „Право и Интернет“	1.12. §27 ЗИД предвижда създаването на чл. 27ж, съгласно който: „Чл. 27ж. (1) При осъществяване на своите правомощия, по отношение на съществените субекти, органите по чл. 27е имат право: 1. да извършват проверки - планови и извънпланови, на място или дистанционни, извършвани от компетентни оправомощени служители; …“Сравнение с чл. 32, параграф 2, буква а) от Директивата („проверки на място или дистанционни проверки, включително случайни, извършвани от обучени специалисти“) показва известно разминаване, което може би е препоръчително да се обсъди допълнително, за да се прецени дали и доколко българският текст му съответства (т.е. дали „компетентни оправомощени служители“	**Не се приема.**	„компетентни оправомощени служители“ - отговарят на определени изисквания за компетентност по длъжностни характеристики.

	съответства на „обучени специалисти“). По отношение на извънплановите проверки („случайни проверки“ по смисъла на Директивата) в този член е препоръчително да се предвидят специални правила, ред и механизъм за извършването им, вкл. дали не е необходим предварителен контрол от съд, сходно на режима, например, по Закона за защита на конкуренцията и други подобни актове. Значителните нови правомощия на компетентните органи предполагат да са налице и съответни процесуални и законови средства за защита на субектите.	**Не се приема.**	До колкото не са предвидени специални правила, следва да се прилагат общите правила за осъществяване на административен контрол, респективно административнонаказателна дейност.
Фондация „Право и Интернет“	1.13. С §29 ЗИД в чл. 29, ал. 3 и 4 се предлага минималната санкция за съществен субект да е в размер от 200 000 лв., респективно 100 000 лв. за важен субект. Считаме, че подобен размер на минималните санкции не е съобразен с и не отговаря на изискванията на чл. 34, параграф 4 и 5 от Директивата, както и на изискванията на чл. 34, параграф 3 от Директивата, защото в производството по определяне на размера и налагането на санкция автоматично се изключва възможността за преценка на елементите по чл. 32, параграф 7 от Директивата и основополагащите принципи на административнонаказателния процес. Така, например, дори за изключително маловажни случаи органите ще могат да наложат санкция не по-малко от 200 000, респ. 100 000 лв. В този	**Приема се.**	

	контекст следва да се държи сметка и за обстоятелството, че в действащото законодателство са много малко нормативните актове, в които дори максималните санкции не надвишават 200 000 лв., поради което предложеният минимален размер се явява непропорционален и в противоречие на изискванията на Директивата. За да може да се проведе пълноценно и законосъобразно административнонаказателното производство размерът на минималните санкции следва да се намали значително или дори изцяло да се премахне. Само така страната ни може да осигури, че санкциите, които се налагат ще са пропорционални, законосъобразни, адекватни на извършеното нарушение и в съответствие с основните принципи на административнонаказателния процес в България. Това е залегнало и в преамбюли 127 до 133 от Директивата. ➢Известна неяснота в текста има и относно размера на максималните санкции, поради което бихме препоръчали да се ревизира.		
Фондация „Право и Интернет“	**1.14.** С оглед разпоредбите на §40 и §41 ЗИД е силно препоръчително да се предвиди преходна разпоредба, че до приемането на тези актове, и в определен срок след това, няма да бъдат налагани санкции на субектите, за да се даде разумен срок на субектите за подготовка (особено в контекста на това, че голяма част от конкретните нови правила ще са разписани именно в тези подзаконови актове). Новите задължения по закона ще изискват сериозен административен и финансов ресурс за привеждане на дейността им с изискванията, поради което е	**Не се приема.**	Директивата не предвижда такъв отлагателен срок. Законовите разпоредби влизат в сила от датата на влизане в сила на закона. Съгласно Директивата, разпоредбите приети в изпълнение на задължението за транспониране следва да започнат да се изпълняват от 18 октомври 2024 г.

	силно препоръчително да има преходен период след определянето им съгласно §41 за субектите, в който да могат да изпълнят всички задължения по закона.		
Фондация „Право и Интернет“	**1.15.** В §41 ЗИД изглежда има техническа неточност, тъй като препраща към §41, т. 1 ЗИД – вероятно се има предвид §40, т. 1, поради което е добре да се коригира.	**Приема се.**	
Фондация „Право и Интернет“	**1.16.** Бихме искали да обърнем внимание и, че §41 ЗИД посочва, че „***административните органи*** *по чл. 16, ал. 1 в срок до 5 месеца от приемането на решението по § 41, т. 1 определят съществените и важните субекти*“. В същото време с §17 ЗИД се предлага чл. 16, ал. 3, т. 8, съгласно който **националните компетентни органи**: *„8. определят съществените и важните субекти съгласно чл. 4а в съответствие с методика, приета от Министерския съвет, и уведомяват министъра наелектронното управление за това. Методиката се приема по предложение на министъра на електронното управление.“* Така се наблюдава терминологично разминаване относно това кой е органът, който ще определи съществените и важните субекти – по §41 ЗИД това са административните органи, определени с решение на Министерски съвет, а по §17 ЗИД това са националните компетентни органи, които се създават **към** административните органи по чл. 16 ЗК. Считаме, че е препоръчително да се направи	**Приема се.**	

	редакция в §41 ЗИД, за да се прецизира текстът и поясни, че субектите се определят от националните компетентни органи.		
Фондация „Право и Интернет“	**1.17.** §42, т. 1 ЗИД се предвижда нова ал. 2а на чл. 16 ЗЕС, която гласи: „*(2а) Национален компетентен орган за субектите по чл. 4, ал. 1, т. 3, буква а) и б) е Комисията за регулиране на съобщенията.*“ ➢ Анализ на текста показва, че е необходима редакция, чрез която да се изясни, че КРС е национален компетентен орган по смисъла на чл. 16, ал. 1 от Закона за киберсигурност. Освен това следва да се добави, че референцията е към чл. 4, ал. 1, т. 3, буква а) и б) от ЗК, като следва да се изтрие и текстът „ал. 1“, тъй като в сегашния си вид чл. 4 от ЗИД няма алинея 1. Примерно предложение: *„(2а) Национален компетентен орган по смисъла на чл. 16, ал. 1 от Закона за киберсигурност за субектите по чл. 4, т. 3, буква а) и б) от същия е Комисията за регулиране на съобщенията.“*	**Не се приема.**	С § 41 от ЗИД на ЗКС се изменя разпоредбата на чл. 21 от ЗЕС като се създава ал. 6: „(6) Комисията е национален компетентен орган за субектите по чл. 4, т. 3, букви а) и б) от Закона за киберсигурност.“ Съгласно чл. 16 от ЗКС, националните компететни органи се определят с Решение на Министерския съвет само в случаите, в които не са определни от специален закон. В настоящия случай това се уржда в ЗЕС и не е необходимо да се преповтаря в ЗКС.
Фондация „Право и Интернет“	**1.18.** По отношение на §43 ЗИД бихме препоръчали да се направи детайлен анализ дали дефинициите от колоната „съответствие“ в приложения I и II отговарят действително на дефинициите от Директивата, за да се избегне ненужно разширяване на обхвата на закона.	**Приема се.**	
Фондация „Право и Интернет“	**1.19.** Няколко допълнителни предложения: ➢ Препоръчително е да се предвидят ясни и прозрачни **процедури и правила, при които**	**Приема се по принцип.**	Чл. 6, ал. 4 от ЗКС предвижда, че редът за водене, съхраняване и достъп до

	субектите ще отпадат от обхвата на закона и ще бъдат заличавани от регистъра по чл. 6, когато вече не отговарят на изискванията (напр. на изискването за размер или ако вече не предоставят услуга в обхвата на закона). Към настоящия момент липсва информация в кой момент и по какъв ред лице, което е било определено като субект, ще излезе извън обхвата на закона. За някои субекти вероятността това да се случи е почти невъзможна, но по отношение на субекти, при които основният критерий е размер на предприятието, това е много вероятно да се случва – дори ежегодно. В този контекст – или в закона, или в Методиката, е би следвало да се включат правила относно заличаването/отписването на вече определени като субекти лица. Негативен сходен пример в тази посока е например дългогодишния проблем в търговския оборот с невписването (поради бездействие на управител на заличаване на обстоятелства в Търговския регистър), поради което е силно препоръчително да има правила в тази насока.		регистъра, се определят с наредбата по чл. 3, ал. 2, НМИМИС.
	➢ Техническа корекция може да се препоръча по отношение на субектите по чл. 4, т. 3, буква „а“, като за същите се използва съществуващата терминология по ЗЕС – предприятие, предоставящо обществени електронни съобщителни мрежи, съответно услуги.	**Не се приема.**	За целите на ЗКС е използвано определнието от Директивата МИС2. Понятията за „Електронна съобщителна услуга“ и „Обществена електронна съобщителна мрежа“ са понятията по смисъла на ЗЕС.
	➢ Относно т. 9 от Допълнителните разпоредби на действащия Закона за киберсигурност бихме искали да отбележим, че дефиницията на „инцидент със значително увреждащо въздействие“ след приемане	**Приема се.**	

	на ЗИД ще е неприложима и би следвало да се отмени изрично (тя е приета исторически на база чл. 6 от Директива МИС 1). В противен случай ще се получи конфликт между тази разпоредба и новата т. 57 от Допълнителните разпоредби на Закона за киберсигурност (§33, т. 3, буква с) от ЗИД), която именно ще се ползва за тълкуване дали е налице инцидент за докладване по новия чл. 24, предложен със ЗИД. ➢ **В ЗИД изглежда липсва понятието на „инцидент“ по чл. 6, т. 6 от Директивата, като сравнение със съществуващата дефиниция на „киберинцидент“ показва, че не е налице съответствие между двете. Това разминаване е особено важно да се отстрани, защото именно в дефиницията на инцидент по Директивата се залагат основните елементи, въз основа на които се преценява дали има събитие в обхвата на закона и вече при съобразяване на новопредложената т. 57 от Допълнителните разпоредби на ЗК – дали е налице значителен инцидент, подлежащ на докладване.** ➢ Моля да отбележите, че липсва и дефиницията на „киберсигурност“ съгласно чл. 6, т. 3 от Директивата. Силно препоръчително е тя да се въведе, тъй като на нея се основават редица разпоредби от закона, вкл. неговият предмет: *„киберсигурност“ означава киберсигурност съгласно определението в член 2, точка 1 от Регламент (ЕС) 2019/881;* ➢ В ЗИД не идентифицирахме и дефиницията на „сигурност на мрежовите и информационните системи“ по чл. 6, т. 2 от Директивата	**Приема се.** **Приема се.** **Приема се.**	➢т т. 9 от Допълнителните разпоредби....57. **от ДР е включено определението на чл.23. т.3 от Директивата: „Значителен инцидент“** е инцидент, който е причинил или е в състояние да причини сериозно оперативно смущение в услугите или финансова загуба за засегнатия субект, или е засегнал или е в състояние да засегне други физически или юридически лица, причинявайки значителни материални или нематериални вреди. **В т.12а добавя:** „инцидент“ означава събитие, което засяга отрицателно наличността, автентичността, цялостността или поверителността на съхранявани, пренасяни или обработвани данни или на

	➢ Относно съществуващите дефиниции по §3, т. 13, 14 и 15 от Допълнителните разпоредби на действащия ЗК, същите след приемане на ЗИД изглежда ще са неприложими. Същото важи и за дефиницията по §3, т. 31 от Допълнителните разпоредби на действащия ЗК. ➢ Сравнение между §3, т. 3 от Допълнителните разпоредби на действащия ЗК и чл. 6, т. 8 от Директивата показва съществено различие между старата и новата дефиниция на „действия при инцидент“, тъй като включва допълнителни действия, а именно: „всякакви действия и процедури, имащи за цел предотвратяването, установяването, анализа, ограничаването или реагирането на инцидент и възстановяването от него“. Това показва, че е препоръчително да се направи изменение за по-прецизно транспониране на дефиницията ➢ Предходното важи и за дефиницията на „риск“ при сравнение между §3, т. 30 от Допълнителните разпоредби на действащия ЗК и чл. 6, т. 9 от Директивата. ➢ Предходното важи и за дефиницията на „уязвимост“ при сравнение между §3, т. 34 от Допълнителните разпоредби на действащия ЗК и чл. 6, т. 15 от Директивата. ➢ Сравнение между §3, т. 28 от Допълнителните разпоредби на действащия ЗК и чл. 6, т. 34 от Директивата показва съществено различие между съществуващата и новата дефиниция на „представител“. Затова е препоръчително да се направи изменение с цел по-	**Не се приема.** **Приема се.** **Приема се.** **Приема се.** **Приема се.**	услугите, предлагани или достъпни чрез мрежови и информационни системи; ➢3) **Виж чл.2 ал.1 от ЗИД на ЗКС** „киберсигурност“ означава киберсигурност съгласно определението в член 2, точка 1 от Регламент (ЕС) 2019/881; Понятиятя са част от процедурите по управление на инциденти и не би било обосновано същите да бъдат отменени. .

	прецизно транспониране на дефиницията, доколкото представителите имат съществена роля в структурата на новия режим. ➢ Сравнение между §3, т. 19 от Допълнителните разпоредби на действащия ЗК и чл. 6, т. 30 от Директивата показва съществено различие между съществуващата и новата дефиниция на „компютърна услуга в облак“. Затова е препоръчително да се направи изменение с цел по-прецизно транспониране на дефиницията, доколкото представителите имат съществена роля в структурата на новия режим. ➢ Сравнение между §3, т. 11 от Допълнителните разпоредби на действащия ЗК и чл. 6, т. 10 от Директивата във връзка с чл. 2, т. 8 от Регламент (ЕС) 2019/881 показва съществено различие между съществуващата и новата дефиниция на „киберзаплаха“. Затова е препоръчително да се направи изменение с цел по-прецизно транспониране на дефиницията. ➢ Ако се възприемат съображенията в началото на този документ, то следва да се отменят изрично и §3, т. 20 и 26 от Допълнителните разпоредби на действащия ЗК.	**Приема се.** **Приема се.** **Не се приема.**	управлявани услуги за сигурност или доставчик на онлайн места за търговия, на онлайн търсачки или на платформи на услуги за социални мрежи, което не е установено в Съюза, и към което, по отношение на задълженията на даден субект съгласно настоящата директива, компетентен орган или ЕРИКС може да се обръща вместо към самия субект; ➢ **приема бележката** Изменя т. 11 от на действащия ЗК и се запазва дефиницията и чл. 6, т. 10 от Директивата „киберзаплаха“. „киберзаплаха“ означава всяко потенциално обстоятелство, събитие или действие, което може да

			навреди, наруши или по друг начин да окаже неблагоприятно въздействие върху мрежите и информационните системи, ползвателите на такива мрежи и системи и други лица;

			Въведено е ново понятие за административен оран, което, с оглед изложените съображения в началото на документа, изключва необходимостта от отмяната на т. 20 и т. 26 от ДР на действащия ЗКС.
Stanimir.ISotirov	Коментар относно чл. 29- размер на санкциите Чл. 29 (3) Съществен субект, който не изпълни задълженията по чл. 22 и чл. 24 се наказва с имуществена санкция от 200 000 лева до 2% от общия световен годишен оборот за предходната финансова година на предприятието, към което принадлежи съществения субект, но не по –малко от 20 000 000 лева. (4) Важен субект, който не изпълни задълженията по чл. 22 и чл. 24 се наказва с имуществена санкция от 100 000 лева до 1,4% от общия световен годишен оборот за предходната финансова година на предприятието, към което принадлежи важния субект, но не по-малко от 14 000 000 лева. Предложение за промяна - трябва да бъдат изведени ясни и точни критерии за размера на санкциите, когато е заложено те да варират в рамките на 1%-100%. В противен случай, органът, който ще определя размера на санкциите ще бъде принуден да взема субективно решение относно размера на	**Не приема.**	Тези санкции са предвидени в Директивата МИС 2, критериите за определяне на санкциите са уредени в Закона за административните нарушения и наказания.

	тези санкции, което от своя страна е предпоставка за навлизането на корупционни практики.		
jasent	Предложения за промяна в Закона за киберсигурност Добавяне на нова алинея към чл. 27 преди чл. 27ж „Националният компетентен орган утвърждава критерии за акредитация на независими органи по оценка на съответствието и одитори, които могат да извършват обективни и безпристрастни проверки за сигурност и редовни и целеви одити по този закон. Тези критерии трябва да включват изисквания за квалификация, опит и независимост на извършващите проверките, както и процедури за мониторинг и оценка на тяхната работа.“ Мотивация На база на променените текстове в Закона за изменение и допълнение на Закона за киберсигурност и Директива (ЕС) 2022/2555 предлагаме да се въведат промени в закона, които да позволяват извършването на обективни и безпристрастни проверки и одити по този закон от трета страна. Очаква се това да подобри качеството и независимостта на проверките за киберсигурност, да подпомогне Компетентния орган при осъществяването на надзора за спазването на закона и да създаде стандарти за независимите одитори и органи.	**Не се приема**	Предлаганата уредба е предмет на регулация от Регламент (ЕС) 2019/881 на Европейския парламент и на Съвета от 17 април 2019 година относно ENISA (Агенцията на Европейския съюз за киберсигурност) и сертифицирането на киберсигурността на информационните и комуникационните технологии, както и за отмяна на Регламент (ЕС) № 526/2013 (Акт за киберсигурността)

	Необходимо е да се внесе яснота по предложения чл. 27ж, ал. 1, т. 2 „да извършват редовни и целеви одити на сигурността, извършвани от независим орган или компетентен орган“. Референция Регламент ЕО 765/2008 на ЕП и на Съвета от 09 юли 2008 г. за определяне на изискванията за акредитация и надзор на пазара във връзка с предлагането на пазара на продукти и за отмяна на регламент ЕИД 339/3 Предложението е съгласувано с експерти от: Европейски цифров иновационен хъб Тракия Българска асоциация по киберсигурност Български съюз на стандартизаторите		
Адвокатско Дружество "Попов,Арнаудови партньори"	С настоящето представяме две групи предложения за изменение на предложения проект, които биха довели до по-добро постигане на заложените законодателни цели. I. Начинът на включване на **административните органи** като задължени лица по смисъла на закона е направен по начин, водещ до необосновано разширяване на приложното	**Приема се.**	

	му поле.Предложеният проект на изменение води до необосновано широк обхват на попадащите в приложното поле на закона субекти. В него се предлага включването на чл. 4, т. 1 –„административни органи“ (§4 ЗИД). Имайки предвид предложеното препращане към АПК, това предложение практически прави адресати на закона огромен брой субекти, които не са предвидени в директивата. Съгласно §1, т. 1 АПК „Административен орган“ е органът, който принадлежи към системата на изпълнителната власт, както и всеки носител на административни правомощия, овластен въз основа на закон включително лицата, осъществяващи публични функции, и организациите, предоставящи обществени услуги. От друга страна, според дефинициите в Закона за електронно управление, „Лица, осъществяващи публични функции“ са нотариусите, частните съдебни изпълнители, държавните и общинските учебни заведения, държавните и общинските лечебни заведения възложителите по чл. 5, ал. 2 -4 от Закона за обществените поръчки, които не са административни органи или организации, предоставящи обществени услуги, и други лица и организации, чрез които държавата упражнява своите функции и на които това е възложено със закон. „Организация, предоставяща обществени услуги“ е всяка организация независимо от правната форма на учредяването ѝ, която предоставя една или повече услуги. „Обществени услуги“ са образователни, здравни, водоснабдителни, канализационни, топлоснабдителни, електроснабдителни, газоснабдителни, телекомуникационни, пощенски, банкови, финансови в т. ч. застрахователни и удостоверителни по смисъла на Регламент (ЕС) No 910/2014 или други подобни		

	услуги, предоставени за задоволяване на обществени потребности, включително като търговска дейност, по повод на чието предоставяне могат да се извършват административни услуги.Прави впечатление, че немалка част от обществените услуги, дефинирани в Закона за електронното управление, се припокриват с услугите от секторите по новите приложения Iи II, което идва да покаже, че логиката би следвало да е те да се включат в приложното поле на закона, когато това е приложимо с оглед спецификата на конкретната услуга, а не на общо основание. Същото важи и за лицата, осъществяващи публични функции, която видно от дефиницията по §1, т. 12 от ДР на ЗЕУ, включва кръг субекти, които изобщо неса предвидени в Директивата, и не са органи на публичната администрация по смисъла на приложение I, сектор 10, член 2, параграф 2, буква f) от Директивата или чл. 2, параграф 5, буква а) от Директивата.На **първо място практическа последица от това може да е в обхвата на новите разпоредби да попаднат абсолютно всички компании и сектори, и то всички да бъдат считани за съществени субекти.** На следващо място предложеният законов текст ще доведе до неясноти кои точно са задължените субекти. Така например, що се отнася **до образователните институции,** от една страна те ще бъдат уредени в чл. 4, т. 6 от закона, а от друга страна, са включени и в дефиницията на организации, предоставящи публични услуги. Практически чл. 4, т. 6 се обезсмисля, заради прекомерно широкия обхват на чл. 4, т. 1. Това ще означава, че в обхвата на закона биха се включили всички образователни институции без значение дали извършват научноизследователски дейности от критично		

	значение или не. Това обаче очевидно влиза в противоречие със замисъла на текста на чл. 4, т. 6. В текста на закона трябва да се намери начин да се изясни, че се включват само образователните институции, извършват научноизследователски дейности от критично значение.Широката дефиниция на административни органи поставя и въпроси, свързани с приложимостта на изискванията на закона по отношение на органите на публичната администрация на местно равнище. Привеждането в съответствие с тези нови правила за тях би изисквала изключително сериозен финансов и административен капацитет, който редица по-малки администрации не биха могли да осигурят. Прекомерното разширяване на обхвата на закона по отношение на тези администрации ще доведе и до липса на консистентност в различните държави-членки.Широката дефиниция на административни органи води до колизия и на нормите на чл. 4, т. 1 и чл. 4, т. 7 и 8. Включването на 7 и 8 е оправдано, ако волята на законодателя е тези групи да попадат в обхвата на закона, **само когато предоставят административни услуги по електронен път.** Ако обаче се възприеме широка дефиниция наадминистративни органи съгласно т. 1, то т. 7 и 8 са излишни.Считаме, че стестняването на обхвата на образователните институции в предложената редакция на чл.4, т.6 също представлява солиден аргумент в подкрепа на подхода за стеснен и хармонизиран обхват, в съответвие с целите и духа на Директива (ЕС) 2022/2555 на Европейския парламент и на Съвета от 14 декември 2022 година относно мерки за високо общо ниво на киберсигурност в Съюза, за изменение на Регламент (ЕС) No 910/2014 и Директива (ЕС)		

	2018/1972 и за отмяна на Директива (ЕС) 2016/1148 (долу „Директивата“), чието транспониране в националното законодателство се цели с обсъжданите тук изменения. Отново заради широката дефиниция на административни органи, свързана със системата от препращания, ще възникнат затруднения и по отношение на онези субекти, при които има припокриване между основното правно основание и дефиницията на административни органи. Това се отнася например за субектите от **сектор „Пощенски услуги“, както и за телекомуникационните, удостоверителните, електроснабдителните** и т.н. услуги. Конкретна последица ще е неяснотата кой ще е националният компетентен орган и на кое основание. Напомняме, че за административни органи национален компетентен орган е Министерство на електронното управление, а за отделните сектори са предвидени отделни различни органи. Обръщаме внимание в тази връзка, че в преамбюла на Директивата НИС2 изрично е посочено, че определени пощенски и удостоверителни услуги не следва да попадат в обхвата на новите регулации.В допълнение към всички изложени съображения относно включването на административните органи в обхвата на закона, следва да се обърне внимание, че Директивата изисква съществени субекти да са само лицата по чл. 2, параграф 1, буква е), точка i) от Директивата, а не всички органи на публичната администрация. В тази връзка е препоръчително да се уточни кои са съществени и кои важни субекти.Предвид изложеното, предлагаме определено ревизиране на текстовете, свързани с административните органи. То ще бъде в съответствие и с преследвания от		

	държавата балансиран подход по транспониране (максимален баланс между заложените в Директивата цели/обхват и местното законодателство) и с оглед постигането на по-високо ниво на хармонизация на ниво ЕС.Този проблем може да бъде коригиран чрез въвеждането на **самостоятелна дефиниция на административен орган в новия закон, а не да се използва препращане към АПК или система от препращания към АПК и ЗЕУ. Предлагаме следната дефиниция: „Административен орган“ е органът, който принадлежи към системата на изпълнителната власт.** В допълнение предлагаме да се уточни, че за целите на прилагане на закона **се изключват органите на местно самоуправление.** С това би се спазило изискването на член 2, параграф 2, буква f) и параграф 5 от Директивата. Директивата предвижда, че тя се прилага към органите на регионално ниво, както е определено от държава членка в съответствие с националното законодателство, когато след оценка, основана на риска се установи, че лицето (органът), предоставя услуги, прекъсването на които би могло да има значително въздействие върху критични социални или икономически дейности. Директивата изрично дава възможност, но не задължава държавите да включват всички органи на местно ниво.При запазване на препращанията и използваните дефиниции препоръчваме изричноизключване на образователните институции от обхвата на закона с оглед избягване на необоснована ресурсна тежест за същите. Считаме, че не случайно образователните институции са изключени от задължителното приложно поле на Директивата, предвид целите, функциите и особеностите		

	на тяхната работа. Без съмнение, включването в приложното поле на закона и, съответно, привеждане на дейността в съответствие с неговите изисквания, би било много голяма тежест и за образователни институции, когато извършват научноизследователски дейности от критично значение. Ако, все пак, се прецени, че образователните институции следва да останат в приложното поле на закона, както са посочени в предложената редакция на чл.4, т.6, **считаме, че е крайно необходимо да се въведе нарочна дефиницияна понятието „научноизследователски дейности от критично значение".** Препоръчваме изрично изключване на органите на изпълнителната власт на местно ниво от обхвата на закона. Препоръчваме и отпадане изцяло на т. 7 и 8 на чл. 4 ЗК, доколкото уредените там субекти, попадат и в дефиницията на административен орган. Следва да се обмисли стесняване на обхвата на самите административни органи до тези по член 2, параграф 1, буква е), точка i) от Директивата, и уточняване кои от тях ще са съществени и кои важни.- приема се		
	II. В предложения чл. 23 се съдържат неясни критерии, които в този вид не гарантират обективност. В чл. 23, ал. 1 от предложения проект е предвидено, че Съветът по киберсигурността идентифицира и прави **оценка на технологичните и нетехнологичните рискове,** като изготвя съгласувано с компетентните органи мотивирано предложение до Министерски съвет да ограничи използването на конкретни технологии или на критични	**Приема се.**	

	вериги за доставка на ИКТ услуги, ИКТ системи или ИКТ продуктови вериги за доставка, за субектите на този закон, доколкото с това не се засягат императивни разпоредби на правото на Европейския съюз или на действащото българско законодателство и не се влиза в противоречие с координираните оценки на риска на ниво Европейски съюз. Министерският съвет се произнася с административен акт, издаден по реда на Административнопроцесуалния кодекс в рамките на предоставените му с действащото законодателство правомощия. В частта, свързана с включване на технологичните и нетехнологичните рискове, текстът влиза в противоречие с предвиденото в директивата. Текстът би следвало да кореспондира на чл. 22 от Директивата. В директивата обаче е посочено, че рисковете могат да бъдат взети предвид, а в българският текст е въведено обвързващо изискване за това. В допълнение, директивата посочва, че нетехнологичните рискове се вземат предвид, когато това е подходящо, а в българския текст такова уточнение не се съдържа. Това би могло дадоведе до разминаване в оценките на риска, правени в България и останалите държави в ЕС. Следва да се отчита и липсата на единна дефиниция по отношение на това какво означава технологични и нетехнологични рискове, което създава опасности при правоприлагането. За да се осигури ефективно внедряване на NIS 2.0, от решаващо значение е координираните оценки на риска да се фокусират върху добре дефинирани и общоприети критерии. Тези критерии трябва да бъдат обективни, недискриминационни и да отразяват стандартите, признати в съответните отрасли. Важно е тези оценки да включват добре дефиниран обхват,		

	който прави разлика между критични и некритични елементи на ИКТ продуктите и услугите, формулирани чрез задълбочени консултации с експерти от индустрията. Затова предлагаме да не се разчита на двусмислени термини като „технически“ и „нетехнически“, а на ясни и обективни критерии. Това би довело до намаляване на потенциалните конфликти в процеса на оценяване.Считаме, че мерки за сигурност, предприемани от всяка една държава, следва да почиват на признати национални и международни стандарти, специфични за сектора, както и стандарти за целия ЕС, когато има такива. Те следва да бъдат предварително и ясно дефинирани и законът да въвежда необходимото позоваване на тях. В тази връзка е важно да се поддържа политика за създаване на унифицирани европейски стандарти, имащи обективни измерители. Важно е да се избегне опасността от политическо и субективно оценяване, каквато би съществувала при използването на израза **„нетехнологични рискове“, който е лишен от конкретно съдържание**. Не е без значение и факта, че в директивата, за разлика от предложения законов текст „нетехнологични рискове“ имат спомагателно и допълващо значение. Използването на ясни и обективни стандарти ще даде надеждни насоки за киберсигурност и по този начин ще насърчава доверието и увереността в цифровата инфраструктура. Налице са и икономически ползи, защото стандартите ще позволят на бизнеса да разбира и прилага необходимите мерки за сигурност по-ефективно, намалявайки икономическите загуби и свеждайки до минимум смущенията поради проблеми със съответствието. Това насърчава икономическата стабилност и растеж. Ще се		

	повиши и правната сигурност, чрез гаранции за последователно и предвидимо прилагане на правилата за киберсигурност. Неоспорима полза от прилагането на стандарти, подлежащи на актуализиране и развитие е и че това позволява да се поддържа постоянна адекватност на критериите за оценка. Правната рамка, основана на обективни стандарти, също така ограничава произволното разширяване на властта на правителството, като гарантира, че властта се упражнява в рамките на конституционните граници и защитава основните права.Предвид изложеното, предлагаме да се обмисли корекция на чл. 23 като от него отпадне оценката на нетехнологични рискове, доколкото това е лишено от конкретика понятие, на което в проекта на закон, за разлика от директивата, се дава водещо значение. – приема се – изменен чл. 23		
Комисията за регулиране на съобщенията	1. В пар. 3 в чл. 3 да се създаде нова ал. 5 със следното съдържание: „Минималният обхват на мерките за постигане на високо общо ниво на киберсигурност и критериите за докладване на инциденти за субектите по чл. 4, , т. 3, буква а), се определят с наредба на Министерския съвет по предложение на Комисията за регулиране на съобщенията и министъра на електронното управление.“ Мотиви: В проекта е предвидено да бъде изготвена наредба, приета от Министерския съвет по предложение на министъра на електронното	**Приема се.**	

	управление. Наредбата следва да обхваща мерките за постигане на високо общо ниво на киберсигурност и критериите за докладване на инциденти за субектите по чл. 4. От обхвата на наредбата са изключени субектите по чл. 4, т. 3, б. „а“ , а именно - субектите от изброени в приложенията към проекта видове, когато услугите се предоставят от доставчици на обществени електронни съобщителни мрежи или на обществено достъпни електронни съобщителни услуги. В тази връзка те не попадат в обхвата на наредбата. Съгласно чл. 243, ал. 3 от Закона за електронните съобщения (ЗЕС), КРС приема Правила за минималните изисквания за сигурност на обществените електронни съобщителни мрежи и услуги и методи за управление на риска за тяхната сигурност (Правила). В Приложение № 1 от Правилата, приети от КРС, се съдържат изисквания за технически и организационни мерки, свързани със сигурността, които предприятията следва да предприемат. Същите са базирани на Насоките на ENISA за мерките за сигурност , съгласно Европейския кодекс за електронни съобщения. Същевременно мерките са съобразени да изпълняват технически мерки ТМ01: Осигуряване на прилагането на базови изисквания за сигурност, ТМ02: Осигуряване и оценка на прилагането на мерките за сигурност в съществуващите 5G стандарти, ТМ03: Осигуряване на строг контрол на достъпа, ТМ05: Осигуряване на сигурни управление, експлоатация и мониторинг на 5G мрежите, ТМ06: Укрепване на физическата сигурност,		

	ТМ07: Укрепване на целостта на софтуера и управлението на актуализациите и кръпките и ТМ08: Повишаване на стандартите за сигурност в процесите на доставчиците чрез стабилни условия за обществени поръчки от Инструментариума на ЕС за киберсигурността в областта на 5G. С проекта на ЗИД на ЗК е предвидено чл. 243 от ЗЕС да бъде отменен, което ще доведе до отпадане на правното основание на което са приети правилата. В тази връзка считаме, че правомощието за приемане на подзаконов нормативен акт следва да бъде законово предвидено. Липсата на подзаконов нормативен акт е първата съществена разлика между съществуващата правна рамки и предложения проект. Считаме съществуващата наредба, съгласно чл. 3, ал. 2 от Закона за киберсигурност за недостатъчна по отношение на електронните съобщителни мрежи и услуги. В нея не се определя изискваната информация, формата и начинът на уведомяване за инцидентите, свързани със сигурността. В тази връзка, считаме, че следва да се предвиди изрично подзаконов нормативен акт, който да урежда мерките за постигане на високо общо ниво на киберсигурност и критериите за докладване на инциденти за субектите по чл. 4, т. 3, буква а). Също така, отделянето на обществените електронни съобщителни мрежи и услуги в самостоятелен подзаконов нормативен акт би улеснило сектора при прилагането му. – приема се – да го отразим		

	2. Във връзка с горното предложение, предлагаме да бъде включено допълнение на § 40 към законопроекта, като се създаде нова т. 3 със следното съдържание: „т. 3. В срок до 8 месеца от влизането в сила на закона приема наредбата по чл. 3, ал. 5. До приемане на Наредбата по ал. 5, се прилагат Правилата, приети на основание чл. 243, ал. 3 от ЗЕС".	**Приема се.**	
	3. В ал. 2 на чл. 3 е посочена неточна препратка към чл. 4, ал. 1, т. 3, б. „а", като следва да отпадне „ал. 1", тъй като проектът предвижда чл. 3 да се състои само от точки. Навсякъде текстът на проекта следва да се коригира в този смисъл.	**Приема се.**	
	4. С оглед яснота, по преценка в чл. 3 ал. 3 да се допълнят думите „по чл. 5, т. 2 не се прилага и наредбата по ал. 5". Мотиви: Уточнението е необходимо във връзка с предложението за наредба, която да се отнася само за обществените електронни съобщителни мрежи и услуги.	**Приема се.**	
	5. В пар. 11 предлагаме в чл. 9, ал. 3 да се създаде нова точка със следното съдържание: „8г. председателят на Комисия за регулиране на съобщенията" Мотиви: В настоящия законопроект е предвидено КРС да е компетентен орган по отношение на субектите на услуги, предоставяни от доставчици	**Не се приема.**	СКС е постоянно действащ консултативен политически орган на ниво МС, в съответствие с позицията и ролята му отредена в

	на обществени електронни съобщителни мрежи или обществено достъпни електронно съобщителни услуги и на услугите от доставчици на удостоверителни услуги. В тази връзка би следвало председателя на КРС да е част от Съвета по киберсигурност. Горното се подкрепя и от разпоредбите на законопроекта, тъй като съгласно пар. 12 от проекта, в чл. 10, т. 6 Съветът предлага на Министерския съвет Национален план за реакция при мащабни киберинциденти и киберкризи, в съответствие с Препоръка (ЕС) 2017/1584 на ЕК от 13 септември 2017 г, относно координирана реакция на мащабни инциденти и кризи. Наред с посоченото, съгласно пар. 19 се създава нов чл. 17а, съгласно който Съветът е компетентният орган, който отговаря за управлението и мащабните киберинциденти и киберкризи. С оглед същественото значение на електронните съобщения и мрежи в случаи на мащабни киберинциденти и киберкризи, както и предвид останалите правомощия на Съвета считаме, че председателят на КРС следва да бъде включен като член на органа.	**Не се приема.**	Стратегията за Киберсигурност СКС координира действията на политическо и стратегическо ниво за гарантиране постигането на необходимите капацитет и способности за киберсигурност. Съветът осигурява сътрудничеството между компетентните държавни органи, какъвто се предвижда да бъде и КРС, бизнеса, академичния сектор, неправителствените организации при определянето и провеждането на държавната политика в областта на киберсигурността. Съгласно действащият Правилник за дейността на СКС в определени случаи и по отделни въпроси в работата на съвета по покана на неговия председател може да участват председатели на постоянни комисии на НС, народни представители и ръководители на ведомства и организации. С § 41 от ЗИД на ЗКС се изменя разпоредбата на чл. 21 от ЗЕС като се създава ал. 6: „(6) Комисията е национален компетентен орган за субектите

	6. По отношение на пар. 17, предлагаме в чл. 16 да се създаде нова ал. 2а със следното съдържание: „Национален компетентен орган за субектите по чл. 4, т. 3, буква а) и б) е Комисията за регулиране на съобщенията“ Мотиви: Предвид пар. 42 считаме, че определянето на КРС като компетентен орган е по-подходящо да се извърши чрез изменение на чл. 16 от Закона за киберсигурност, като бъде добавена изрична разпоредба, която да предвижда, че КРС е Национален компетентен орган за субектите по чл. 4, т. 3, буква а) и б). В случай че описаният подход не бъде възприет и КРС се определи за компетентен орган чрез изменение на специалния закон (ЗЕС), считаме, че следва да бъде изменен чл. 30 от ЗЕС, като се създаде нова т. 30 в ал. 1. „осъществява функциите на национален компетентен орган за субектите по чл. 4, т. 3, буква а) и б) от Закона за киберсигурност“ 7. По отношение на § 28 от Законопроекта: В чл. 27е, ал. 2 предлагаме прецизиране на текста, както следва: „За осъществяване на контрол по този закон ръководителите на съответните органи по ал. 1 оправомощават със заповед служители от техните администрации.“ 8. По отношение на § 29 от Законопроекта:	**Приема се.** **Приема се.**	по чл. 4, т. 3, букви а) и б) от Закона за киберсигурност.“ Съгласно чл. 16 от ЗКС, националните компететнти органи се определят с Решение на Министерския съвет само в случаите, в които не са определни от специален закон. В настоящия случай това се уржда в ЗЕС и не е необходимо да се преповтаря в ЗКС.

	В чл. 28 е предвидено налагането на глоба на административен орган, който не изпълни принудителна административна мярка по смисъла на чл. 27и, ал. 1, т. 2 – т. 7. Предлагаме прецизиране на текста с оглед разпоредбите на ЗАНН и възможността за налагане на имуществена санкция. Мотиви: С оглед факта, че глоба може да бъде наложена само на физическо лице, в случай че административният орган не е физическо лице, а юридическо, по отношение на него следва да се наложи имуществена санкция; Ако административният орган по чл. 28 от Законопроекта може да е и юридическо лице, предлагаме освен глобата, в ал. 1 и 2 да се добави и имуществена санкция; ако административният орган по чл. 28 от Законопроекта може да бъде само физическо лице, предлагаме това да се уточни изрично в двете алинеи на разпоредбата. 9. По отношение на § 29 от Законопроекта, предлагаме текстът на чл. 29, ал. 2 да придобие следната редакция: „(2) Имуществените санкции се налагат независимо от наложените мерки, посочени в чл. 27и, ал. 1“, както и да се прецизират препратките. Мотиви: В чл. 29, ал. 2 е направено препращане към чл. 27и, ал. 1, т. 2 от б. б) до б. ж); в чл. 29, ал. 2 е предвидено, че „..имуществените санкции се налагат в допълнение към която и да е от мерките,	**Приема се.**	

	посочени в чл. 27и, ал. 1, т. 2 от б. б0 до б. ж)“. Член 27и, ал. 1, т. 2 не съдържа букви от „б“ до „ж“. На следващо място, от текста на разпоредбата става ясно, че имуществените санкции се налагат в допълнение към съответните мерки по чл. 27и, т.е., за да бъде наложена санкцията, е необходимо първо да има наложена мярка по чл. 27и. Същевременно, в чл. 29, ал. 5 е предвидено, че освен имуществената санкция по ал. 3 и ал. 4, на съществените и важните субекти могат да бъдат налагани и една или няколко от мерките по чл. 27и и чл. 27к. Считаме, че във всеки случай на нарушение на закона, следва да се налага имуществена санкция, независимо от това дали компетентният орган ще наложи мярка по реда на чл. 29, ал. 5 от Законопроекта. Тази санкция не следва да е допълнение към мярката, тъй като не може да бъде обусловена от нейното налагане, още повече, че органът може да реши да не наложи такава мярка. 10. По отношение на § 29 от Законопроекта, предлагаме в чл. 29, ал. 6 да се прецизира текстът, като се предвиди възможността за налагане на глоби Мотиви: В Законопроекта е предвидено, че при нарушение на чл. 21, управителите или членовете на управителните органи на съществените и важните субекти подлежат на имуществена	**Приема се.**	

	санкция в размер на 1000 лв. до 100 000 лв. Управителите или членовете на управителните органи, когато са физически лица, не могат да бъдат наказвани с имуществени санкции, а с глоби (арг. от чл. 83, ал. 1 от ЗАНН). Имуществената санкция е приложима само когато член на управителен орган е юридическо лице. Предлагаме текстът да се прецизира, с оглед разпоредбите на Търговски закон и останалото приложимо законодателство Редакционни бележки: 11. В пар. 24 считаме, че в чл. 21 следва да се включат и административните органи предвид това, че попадат в обхвата чл. 4а, ал. 1, т. 4, като съществени субекти. 12. Пар. 28: Чл. 27к, ал. 5, изр. 1, 2 и 3 следва да се редактират, тъй като се въвежда неясна формулировка относно физическите лица, които могат да бъдат подведени под отговорност. 13. Да се допълни § 35 от проекта „До 17 януари 2025 г. националните компетентни органи предоставят информацията по чл. 6 на министъра на електронното управление“, тъй като за субектите по чл. 4 и 4а не е посочен срок за предоставяне на информацията по чл. 6 на националните компетентни органи. В чл. 6 единствено е определен срок за предоставяне на информация при промяна на вече предоставени данни.	**Приема се.**	

	14. Пар. 40 препраща към Методика по чл. 4, ал. 3. Текстът не кореспондира, т.к. чл. 4 няма алинеи и не предвижда приемането на методика. Вероятно се има предвид методиката по чл. 16, ал. 3, т. 8. 15. Пар. 41 – препратката следва да е към пар. 40, т. 1.		
Алиансът на технологичната индустрия (ATI)	Становище на Алианса на технологичната индустрия по проект на Закон за изменение на Закона за киберсигурност(Проект) 1. По §3 от Проекта -Предложение за създаване на нова ал. 3 на чл. 3, в два, алтернативни варианта, както следва: 1.1. „(3) Мерките за постигане на високо общо ниво на киберсигурност за субектите по чл. 4, т. 3, буква „а“, се определят в правилата за минималните изисквания за сигурност на обществените електронни съобщителни мрежи и услуги и методи за управление на риска за тяхната сигурност, приети от Комисията за регулиране на съобщенията по реда на Закона за електронните съобщения. Останалите алинеи на чл. 3 се преномерират съответно.Във връзка с горепосоченото предложение, допълнително предлагаме (тук, макар	**Приема се.**	

	и несистематично от гл. т. структурата на ЗИДЗКС, но с цел яснота и проследимост) в § 42 от Проекта, т. 4 буква б) да се измени както следва:„б) В раздел I чл. 243б, чл. 243в, чл. 244 и чл. 244а се отменят.“ 1.2 В случай че не приемете предложението за промяна по т.1.1., алтернативно предлагаме създаване на нова ал. 3 в чл. 3, от Проекта със следния текст: „(3) Мерките за постигане на високо общо ниво на киберсигурност за субектите по чл. 4, т. 3, буква „а“, се определят в правила за минималните изисквания за сигурност на обществените електронни съобщителни мрежи и услуги и методи за управление на риска за тяхната сигурност, приети от Комисията за регулиране на съобщенията. Правилата се приемат след провеждане на обществено обсъждане и се обнародват в „Държавен вестник“. При изготвянето и приемането 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.“Останалите алинеи на чл. 3 се преномерират съответно.Във връзка с горепосоченото алтернативно предложение, допълнително предлагаме		

	(тук, макар и несистематично от гл. т. структурата на ЗИДЗКС, но с цел яснота и проследимост) в § 42 от Проекта, т. 4 буква б) да се измени както следва:„б) раздел I се отменя след приемането на предвидените в чл. 3 нормативни актове относно определяне на минималният обхват на мерките за постигане на високо общо ниво на киберсигурност.“.Мотиви:Член21, пар. 2 от Директива МИС 2, предвижда задължение за държавите членки да приемат по отношение на съществените и важни субекти подходящи и пропорционални технически и организационни мерки за управление на рисковете за сигурността на мрежовите и информационни системи. В настоящия Проект, това задължение е отразено с разпоредбата на чл. 3, според която минималните мерки за постигане на високо ниво на киберсигурност се определят с наредба, издадена от Министерски съвет по предложение на министъра на електронното управление. От съдържанието на наредбатакато задължени лица са изключени субектите по чл. 4, ал. 1 т. 3, буква а), а именно доставчицитена електронни съобщителни мрежи и електронни съобщителни услуги. Считаме това за съществена празнина, която поставя в неяснота мерките,които следва да се приемат и прилагат от доставчици на електронни съобщителни мрежи и/или електронни съобщителни услуги. Към настоящия момент посочените субекти прилагат техническите и организационни мерки, приети с Правила за минималните изисквания за сигурност на обществените електронни съобщителни		

	мрежи и услуги и методи за управление на риска за тяхната сигурност -приети на 19.05.2022 г. (Правилата). С тях се определят минималните изисквания за сигурност на обществените електронни съобщителни мрежи и услуги и методите за управление на риска за тяхната сигурност. Правилата изпълняват предвидените в чл. 21, пар.2 от Директива МИС 2 минимални мерки, като се съобразяват с последните постижения в областта на киберсигурността, които са в съответствие с приложимите стандарти в тази сфера. На това основание и поради факта, че настоящия Проект, определя КРС като Национален компетентен орган (НКО) за доставчицитена електронни съобщителни мрежи и електронни съобщителни услуги считаме за уместно Правилата да запазят своята приложимост и при транспонирането на Директива МИС2 в националното законодателство. Даденото предложените отговаря и на посоченото в съображение 95 от Директива МИС 2условие, че „когато е целесъобразно и за да се избегнат ненужни смущения, съществуващите национални насоки, приети за транспониране на правилата, свързани с мерките за сигурност по членове 40 и 41 от Директива (ЕС) 2018/1972, следва да се вземат предвид при транспонирането на настоящата директива, като по този начин се надгражда върху вече придобитите знания и умения съгласно Директива (ЕС) 2018/1972 относно мерките за сигурност и уведомленията за инциденти.“В тази връзка смятаме за целесъобразно приетите от КРС на основание чл. 243, ал. 3, изр.		

	първо от Закона за електронните съобщения (ЗЕС) Правила за минималните изисквания за сигурност на обществените електронни съобщителни мрежи и услуги и методи за управление на риска за тяхната сигурност да бъдат запазени, като при необходимост бъдат изменени и допълнени с цел пълно съответствие с ДирективатаМИС 2.Също така предложението ни е съобразено с изискването за „равностоен ефект“ на задълженията, предвидено в чл. 4, пар. 2, б. „а“ и „б“ от Директива МИС2, като допълнително отчита и Насоките на Комисията относно прилагането на чл. 4, параграфи 1 и 2 от Директивата, в т. II.1.6, вкоито е изрично е посочено, че ако специфичните секторни изисквания са подробни или по-детайлни от тези по Директива МИС 2, трябва да се прилагат последните.2. По§11 от Проекта –предлагаме да бъде създадена нова т. 19в чл.9, ал. 2от Закона за киберсигурност със следното съдържание: „19. председателят на Комисията за регулиране на съобщенията.“Мотиви: Включването на председателя на Комисията за регулиране на съобщенията в Съвета по киберсигурност отчита факта, че в обхват на чл. 9а на Директива (ЕС) 2022/2555 вече попада и секторанаелектроннитесъобщителнимрежииуслуги. Гарантирането на поддържането на сигурността на мрежите и услугите е една от водещите цели на ЗЕС (чл. 4, ал. 1, т. 4, б. „в“), респ. попада в общите законови правомощия на КРС, която по закон осигурява	**Не се проиема.**	СКС е постоянно действащ консултативен политически орган на ниво МС, в съответствие с позицията и ролята му отредена в Стратегията за Киберсигурност СКС координира действията на политическо и стратегическо ниво за гарантиране постигането на необходимите капацитет и способности за киберсигурност. Съветът осигурява сътрудничеството

	спазването на изискванията за поддържане на целостта на обществените електронни съобщителни мрежи и за сигурност на обществените електронни съобщителни мрежи и услуги и разследва случаи на неспазване на изискванията за осигуряване на сигурност на обществените електронни съобщителни мрежи и услуги, както и въздействието им върху сигурността на мрежите и услугите, като при необходимост си съдейства с компетентните органи по чл. 244а, ал. 3 (чл. 30, ал. 1, т. 22 от ЗЕС).Допълнително, предложението е в съответствие със съображение 95 от Преамбюла на МИС2, посочено по-долу, като отчита и секторната компетентност на КРС на специализиран независим държавен орган, който осъществява функциите по регулиране и контрол при осъществяването на електронните съобщения в Република България(чл. 21, ал. 1 и ал. 2 от ЗЕС). По §16 от Проекта -предлагаме разпоредбата на чл. 15, ал. 7 от Проекта да отпадне.Мотиви:Разпоредбата на чл. 15, ал. 7 от Проекта предвижда създаване на автоматизиран механизъм за обмен на информация, между ръководителите на стратегически обекти и възлагащите и извършващите стратегически дейности от значение за националната сигурност сДържавна агенция национална сигурност (ДАНС). Въпросното задължение излиза извън обхвата на Директива МИС2 на първо място с оглед съображение 24 от нея, съгласно което автоматизиран обмен на информация е предвиден след преценка за	**Не се приема.**	между компетентните държавни органи, какъвто се предвижда да бъде и КРС, бизнеса, академичния сектор, неправителствените организации при определянето и провеждането на държавната политика в областта на киберсигурността. Съгласно действащият Правилник за дейността на СКС в определени случаи и по отделни въпроси в работата на съвета по покана на неговия председател може да участват председатели на постоянни комисии на НС, народни представители и ръководители на ведомства и организации. Чрез ЗИД на ЗКС се обективира работата на Център за мониторинг и реакция на инциденти със значително увреждащо въздействие върху комуникационните и информационните системи на стратегическите обекти и дейности, които са от значение за националната сигурност, която предвижда

	целесъобразност и с оглед осъществяване на автоматично докладване на съществени инциденти по реда на чл. 24 от Проекта. С оглед на това и задълженията по Директива МИС2, въведената възможност за изграждане на механизъм за автоматично докладване на съществени инциденти следва да се изгради между съществените и важни субекти и компетентнитеоргани (или СЕРИКС), до които е предвидено да се извърши докладване на инцидент. Разпоредбата на чл. 15, ал. 7 или други разпоредбив Проекта не предвиждат функция на ДАНС, в рамките на която да получава доклади за възникнали инциденти при съществените и важни субектипо смисъла на Директива МИС2. Въпросната разпоредба е дефинирана общо, като не дава конкретика каква информация следва да се обменя, технологията с помощта на която следва да се извършва този обмен и не представя гаранции за защита от разпространение на чувствителна информациядо трети лица. Всичко това не позволява на задължените субекти да направят преценка, относно финансовите инвестиции, които следва да направят за осъществяването на автоматичния обмен на информация, което застрашава цялостното му въвеждане. Следователно,в Директивата няма предвидено правно основание за въвеждане на подобен механизъм за автоматизиран обмен с органите в областта на националната сигурност. В допълнение следва да се посочат и чл. 2, пар. 6 и 7 от МИС 2, както самият ЗИДна ЗКС, който в чл. 7, т. 3 предвижда, че		автоматизиран обмен на информация между ръководителите на стратегически обекти и възлагащите и извършващите стратегически дейности от значение за националната сигурност с Центъра. С развитието на технологията се увеличава процесът на автоматизация и споделяне на информация за инциденти.

	„този закон не се прилага... по отношение на информационните системи, дефинирани като критични в стратегически обекти или субектите, осъществяващи стратегически дейности, определени от ръководителите на стратегическите обекти и възлагащите стратегически дейности, които са от значение за националната сигурност, по смисъла на Наредбата за условията и реда за определяне на мерките за защита на информационните и комуникационните системи на стратегическите обекти от значение за националната сигурност и за осъществяването на контрол“. Тоест в самия Законопроект е въведено изрично нормативно изключениев тази посока. По §20 от Проекта -предлагаме следната редакция на чл. 18, ал. 1 от Проекта:Чл. 18 (1) Националните компетентни органи по смисъла на този закон, създават секторни екипи за реагиране при инциденти с компютърната сигурност (СЕРИКС). Екипите се създават към националните компетентни органи в съответствие с методическите указания на Агенцията на Европейския съюз за киберсигурност (ENISA). Мотиви: Разпоредбатана чл. 18, ал. 1 от Проекта, предвижда задължение за Националните компетентни органи (НКО) да създадат СЕРИКС в рамките на техните организации. НКО по смисъла на Проекта са посочени не само в разпоредбата на чл. 16, ал. 1, но и в	**Приема се.**	С оглед промяната в чл. 16 целта се постига и не е необходимо да се прави изменение на чл. 18, ал. 1.

	други разпоредби –пр. §42, т. 1, от Преходните и заключителни разпоредби (ПЗР) на закона и който препраща към Закон за електронните съобщения (ЗЕС) и съгласно който НКО за субекти по чл. 4, ал. 1, т. 3, буква а) и б) е Комисията за регулиране на съобщенията. Предходния текст на разпоредбата, създаваше неяснота кои от дефинираните в Проекта НКО следва да създадат СЕРИКС. Това от своя страна създава правна неяснота по отношение на изпълнение на други задължения, предвидени по Проекта –пр. докладване на значителни инциденти от съществени и важни субекти по смисъла на чл. 24 от Проекта, където е предвидено докладване към съответния СЕРИКС, към секторния НКО. 6.По §24 от Проекта 6.1. Предлагаме чл. 23 от Проекта да отпаднеМотиви: Съгласно чл. 22 от Директива МИС 2 оценката на риска за сигурността на критични вериги за доставка се извършва координирано на равнище на Европейския съюз от отГрупата за сътрудничество, заедно с Комисията и ENISA (чл. 22, пар. 2 от Директивата),не от национални органи. С предложения чл. 23 от Проекта некоректно се разширяват правомощията на органи на национално ниводаидентифицират и правят оценка на технологичните и нетехнологичните рискове и да ограничават използването на конкретни технологии или на критични вериги за доставка на ИКТ услуги, ИКТ системи или ИКТ продуктови вериги за доставка, което съществено се отклонява от	**Приема се.**	

	изискванията на Директивата.Въвеждането на подобен национален механизъм,паралелно на **предвидения в Директивата,създава два различни правопорядъка, което противоремина заложенияв Директивата принц**ип за координирана оценка на общностно ниво.6.2.В случай, ве предложението ни по т. 6.1. не бъде прието, алтернативнопредлагаме следната редакция на чл. 23 (1) от Проекта:„Чл. 23 (1) Съветът по киберсигурността идентифицира и прави оценка на технологичните и нетехнологичните рискове, като изготвя съгласувано с компетентните органи и съществените и важни субекти мотивирано предложение до МС да ограничи използването на конкретни технологии или на критични вериги за доставка на ИКТ услуги, ИКТ системи или ИКТ продуктови вериги за доставка, за субектите на този закон, доколкото с това не се засяга правото на Европейския съюз и е в съответствиес координираните оценки на риска наниво ЕС. МС се произнася с административен акт, издаден по реда на Административния процесуален кодекс в рамките на предоставените му с действащото законодателство правомощия.“Мотиви:Съображение 90 от Директива МИС 2 предвижда подход, при който да се отговори на рисковете по веригата за доставка и да се подпомогнат съществените и важни субекти, упражняващи дейности регламентирани по директивата, правилно да управляват веригите на доставки и свързаните с техните доставчици рискове. За целта групата за сътрудничество (чл. 14 от Директива МИС2) заедно с		

	Комисията и ENISA и когато е целесъобразно след консултация със заинтересованите лица, включително от промишлеността, изготвя координирани оценки на риска. Подобен подход беше предприет при приемането на Препоръка (ЕС) 2019/534 наЕвропейскатаКомисията (Киберсигурност на 5G мрежите). Считаме, че подобен подход следва да бъде възприет и в чл. 23 (1) от Проекта, тъй като по този начин ще се установят за всеки сектор кои са критичните ИКТ услуги, ИКТ системи или ИКТ продукти, относимите заплахи и уязвимости. В допълнение, това ще доведе до намаляване на риска от ограничаване на използването на критични компоненти в системите на задължените субекти, което ще доведе до негативно засягане на тяхната икономическа дейност. На следващо място разпоредбата на чл. 23 (1) от Проекта предвижда ограничаването и на определени технологии след извършването на съответните оценки от Съвета по киберсигурност. Това е в противоречие с предвиденото в чл. 22 от Директива МИС2, който определяпо-тесен обхват на Координираните оценки от Групата по сътрудничество (ИКТ услуги, ИКТ системи или ИКТ продуктови вериги за доставка). Представения в проекта вариант излиза извън обхвата на Директива МИС2, като обезсмисля предвиденото съответствие с Координираните оценки на групата по сътрудничество и създава забрана извън пределите на Директивата. В допълнение,считаме че уточнението „или на действащото българско законодателство“, включено в		

	предложения текст на чл. 23, ал. 1 от Проекта е ненужно, доколкото този въпрос е уреден в чл. 15, ал. 1 от Закона за нормативните актове, поради което предлагаме да отпадне 6.3. Предлагаме следната редакция на чл. 24, ал. 2 от Проекта: „(2) Засегнатите субекти уведомяват,когато е подходящо,получателите на техните услуги за значителни инциденти, които има вероятност неблагоприятно да засегнат предоставянето на тези услуги. При изключителни обстоятелства, когато уведомяването им може да изложи на риск разследването на значителния инцидент, насубектите се разрешава, след получаване на съгласие от страна на националния компетентен орган, да забавят уведомяването на получателите, докато националния компетентен орган счете, че е възможно да уведоми за нарушаването на сигурността на лични данни в съответствие с настоящия член.“Мотиви:Предложеният с Проекта текст на чл. 24, ал. 2 е в противоречие с Директива МИС2, в която е предвидено, че получателите на услугите на засегнатите от инцидента съществени и важни субекти следва да бъдат уведомени за инцидента, засягащ ползваните от тях услуги, само когато е подходящо. Противното предвижда съществена административнатежест за съществените и важни субекти, които ще бъдат задължени да докладват за всеки един инцидент, засягащ ползвателите на техните услуги, без да се взима предвид въздействиетона	**Приема се.**	

	инцидента и броя засегнати потребители. 6.4. Предложение по отношение на разпоредбата на чл. 25 от Проекта. 6.4.1. В чл. 1, ал 1 „НКО“ да бъде заменено със „Съвета по киберсигурност“ 6.4.2.По-точно посочване относно какви ИКТ продукти, ИКТ услуги и ИКТ процедури следва да бъдат използвани при поискване от НКО. Мотиви:Предвиденото законово правомощие за изискване с цел доказване на съответствието с конкретни изисквания по чл. 22, от съществените и важните субекти да използват конкретни ИКТ продукти, ИКТ услуги и ИКТ процедури, които са разработени от тях или са придобити от трети страни, сертифицирани в рамките на европейските схеми за киберсигурност, приети съгласно член 49 от Регламент (ЕС) 2019/881 е съществено и следва да се упражнява не от НКО, а на централно ниво от Съвета по киберсигурност.В допълнение разпоредбата на чл. 25, ал. 1 от Проекта представя директно транспониране на чл. 24 от Директива МИС2. Посочената разпоредба е дефинирана общо, без да се съобразятс определени специфики. На първо място липсва конкретизация за какви ИКТ продукти, ИКТ услуги и ИКТ процедури следва да бъдат използвани от съществените и важни субекти при поискване от НКО. С оглед фактът, че Директива МИС 2, както и Проекта на ЗК обхваща широк кръг от субектисъс съществено значение за	**Не се приема.**	Съветът по киберсигурността е консултативен орган, НКО за съответния сектор познава в детайли дейността на сектора и на оперативно ниво, поради което считаме, че е по-целесъобразно той да изиска от съществените и важните субекти да използват конкретни, доказано подходящи в оперативно и икономическо отношение ИКТ продукти, ИКТ услуги и ИКТ процедури, които са разработени от тях или са придобити от трети страни, сертифицирани в рамките на европейските схеми за киберсигурност, приети съгласно член 49 от Регламент (ЕС) 2019/881 на Европейския парламент и на Съвета от 17 април 2019 година относно ENISA (Агенцията на Европейския съюз за киберсигурност) и сертифицирането на киберсигурността на информационните и комуникационните технологии, както и за отмяна на Регламент (ЕС) № 526/2013 (Акт за киберсигурността) (ОВ, L 151 от 7 юни 2019 г.).

	икономиката, промишлеността и обществения живот считаме, че такава конкретизация е необходима да бъде въведена на национално ниво за всяка една категория от задължени субекти по Директива МИС 2.На следващо място следва да бъде представена по-детайлна конкретика относно приложимите (настоящи и бъдещи) национални и европейски схеми за сертификация, които ще се приложимиза съответнитеИКТ продукти, ИКТ услуги и ИКТ процедури, използвани от съществените и важни субекти. Това е необходимо с оглед изпълнението на делегираните актове предвидени по чл. 24, параграф 2 от Директива МИС 2 и възможността за прилагане на чуждестранни схеми за сертифициране. Предложената промяна е в съответствие с чл. 24 от Директивата, като допълнително представлява логично и нормативно продължение на чл. 10 от ЗКС, предвиждащ редица съществени законови правомощия именно на Съвета по киберсигурност, като например: предлагане на МС Национална стратегия за киберсигурност и пътната карта към нея (т. 2); даване предложения за хармонизиране и координиране на секторните политики за постигане на високо общо ниво на киберсигурност на икономиката и обществото (т. 5); предлагане на Национален план за реакция при мащабни киберинциденти и кризи (т. 6) и т.н.7. По §29 от Проекта –предлагаме в чл. 29, ал. 3, 4 и 6 да бъдат премахнати долните граници на предвидените нови имуществени санкции за съществените и важните	**Приема се частично.**	

	субекти, респ. за управителите или членовете на управителните им органи.Мотиви:Разпоредбата на чл. 34 от Директива МИС 2, предвижда общите положения при налагане на административни наказания за нарушения на националнитеразпоредби, приети на основание Директива МИС2. В посочената разпоредба от Директива МИС2 са предвидени, че при транспониране на Директивата следва бъдат съблюдаванипринципите на пропорционалност, ефективност и възпиращ ефект.Директива МИС 2 не предвижда минимални прагове на наложените санкции, както и санкции по отношение на управители и членове на управителни органи. Осъзнаваме необходимостта от налагане на възпиращи мерки срещу нарушение на разпоредбите транспониращи Директива МИС2, но Проекта следва да съобрази размерите на субектитеи икономическите им възможности, тъй като в противен случай се нарушава заложения в Директива МИС2 и чл. 29, ал.1 от Проекта принцип на пропорционалност. Предвид гореизложеното,предлагаме в чл. 29, ал. 3, 4 и 6 да бъдат премахнати долните граници на предвидените нови имуществени санкции за съществените и важните субекти, респ. за управителите или членовете на управителните им органи. Предвидената минимални имуществени санкции (от 200 000 лв.за съществените субекти, например) са прекомерни и необосновании по никакъв начин не отговарят на изискванията на МИС 2 (чл. 34, пар. 1), а и на самия ЗИДЗКС (чл. 29, ал. 1) да бъдат „ефективни, пропорционални и възпиращи“. Подобни прекомерни санкции		В ЗИД на ЗКС са намлени размирите на предвидените санкции, включително и минималните им размери.

	допълнително: драстично ограничават оперативната самостоятелност на административните органи по чл. 16, ал.1 като административнонаказващи органи; представляват механично намаление на минималния размер на максималния праг по МИС 2; необосновано се прилагат генерално за всякакви видове потенциални нарушения на задълженията по чл. 22 и чл. 24 от Законопроекта, които в редица случаи биха били, ако не малозначителни, то с изключително ниска степен на обществена опасност, която по никакъв начин не оправдава налагането на имуществена санкция от минимум 200 000 лв. 8. По §42 -В случай, че не се приеме нито едно от предложенията ни по т. 1 от настоящото становище, предлагаме § 42, т. 4, буква б) от Преходните и заключителни разпоредби на Проекта да се допълни със следния текст: „б) раздел I се отменя след определяне на минималният обхват на мерките за постигане на високо общо ниво на киберсигурност по чл.3.“Мотиви: Предложената разпоредба има за цел да избегне създаването на нормативна празното по отношение на минималните изисквания за сигурност на обществените електронни съобщителни мрежи и услуги и методи за управление на риска за тяхната сигурност, в периода до определяне на минималният обхват на мерките за постигане на високо общо ниво на киберсигурност.		

Васил Грънчаров експерт по киберсигурност	**1.ОБЩИ БЕЛЕЖКИ** Проектът на ЗИД на ЗКС е разработен, без наличието на Национална стратегия за киберсигурност. Последната такава е с изтекъл срок на актуалност на 31.12.2023 г. Същата е разработена през 2021 г., преди да са приети комплекта документи по киберигурност, след 2019 г. Предвид съдржащите се в чл.7, изисквания за минимално необходимото съдържание на Националната стратегия за киберсигурност и поради логиката съпътстваща разработването на регулаторни документи изискваща първоначално да се разработят стратегическите документии след това регулаторните, предлагам Да се разработи първо Национална стратегия за киберсигурностна Република България, а след това да се разработи ЗИД на ЗКС. Това ще даде възможнот посочените в стратегията въпроси по киберсигурноста и релевантни на структурата на закон да бъдат взети предвид: - Непоследователно и несистематично (за съжаление съществен негативен принос за това има и самата ДМИС 2) се използват понятията – „киберсигурност“; „мрежова и информационна сигурност“; „противодействие на киберпрестъпността“ и „киберотбрана“. В чл.2, ал2 на проекта на ЗИД на ЗКС е посочено, че	**Приема се.**	на предприетите от административния орган мерки, според правомощията описани в глава втора „в“и глава трета и дава задължителни предписания за тяхното подобряване. В обхвата на проверките не попадат информационни системи на ведомствата по чл. 5;

	киберсигурността включва, мрежова и информационна сигурност, противодействие на киберпрестъпността и киберотбрана (в ЗИД на ЗКС съгласно Стратегия на ЕС за киберсигурност за цифровото десетилетие приета на 16 декември 2020 г., следва да се включи и кибердипломация). Тези взаимовръзки между трите компонента на киберсигурността от една страна и самата киберсигурност не са отчетени в Проекта. Това създава предпоставка за хаос и объркване. Така например в чл;12, т.5, т.6, т.7 и т.8, на министъра на електронното управление се възлагат отговорности в сферата на киберсигурността, т.е. и областта на противодействие на организираната престъпност и в областта на киберотбраната. Това е в противоречие с чл.12, т.1, с чл.13, ал. и ал.4, т.3. Има противоречие и между чл.27, ал.2 и чл.12, т7. С оглед на наличните неясноти породени поради неточното използване на терминологията и в разрез с разпоредбите предвидени в чл.2, ал.2, е необходимо авторите на Проекта внимателно да прегледат цялостно текстовете му и да ги (особено онези от тях, с които се заменят думите „мрежова и информационна сигурност“ с думата „киберсигурност“). В случай на необходимост да се направят консултации с ЕК ; Пропуски има при определянето на субектите в чл.4.“Обхват“. Взета е прадвид преди всичко ДМИС 2. Проектът не включва текстове отнасящи до важни компоненти от кибирсшгурността.Тези компоненти са залегнали в приети на ниво ЕС регламентиращи документи.. Такива напимер са Регламент(ЕС) 2022/2554 на Европейски парламент и на Съвета от 14 декември	**Не се приема.**	

	2022 година, относно оперативнатустойчивост на цифровите технологии във финансовия сектор (DORA) с него се установяват единни изисквания за сигурност на мрежите и информационните системи, които поддържат работните процеси на над 20 вида финансови субекти. Макар и да има някой общи черти с ДМИС 2, Регламентът съдържа и доста спецфични изисквания. Не са включени основните положения относно определената рамка за сертифициране на киберсигурността. Рамката има за цел да се гарантира подходящо ниво на киберсигурност на ИКТ продукти, ИКТ услуги и ИКТ процеси в Съюза. По аналогичен начин стои и въпросът с Регламент(ЕС) 2021/887 на Европейския парламент и на Съвета от 20 май 2021 година за създаване на изследователски центрове, Европейски център за промишлени, технологични и изследователски експертни познания в областта на киберсигурността и на мрежата от национални координационни центрове. Регламентът предвижда освен създаването на европейския и на националните центрове и правилата за определяне на кандидатури на национални координационни центрове, както и правилата за създаване на експертна общност в сферата на киберсигурността. В българското законодателство съществуват практика за транспониране на евродейски регламенти ш не би трябвало да има пречка основните моменти от тези Регламенти на ЕС да намерят място в Проекта на ЗИД на ЗКС. Така ще се разшири обхватът на ЗКС с важни за националната система за киберсигурност компоненти.Наред с това, ще се избегне явна		Предлаганите изменения не са в обхвата на Директивата МИС 2. Те са предмет на уредба Регламет ЕС 2554/2022.

	неравнопоставеност и справедливост между субектите попадащи в обхвата на ЗКС и финансовте субекти по Регламента. Ако за съществените субекти се предвиждат санкции не по-ниски от 200000 лв. , то за финансовите субекти в чл.52 на Регламента не се предвиждат имуществени санкции. такива - Друг проблем свързан с обхвата на Проекта на ЗИД на ЗКС е свързан с текста по чл.4 ал.1. В него (както между впрочем е и в ДМИС 2), към субектите, които се класифицират като съществени или важни няма изисквания относно наличието на мрежи и информационни системи в субекта имащи значение за основната му дейност. Предлагам по този въпрос да се направи консултация с Групата за сътрудничество.; - В чл.3, ал.4 е предвидено субектите да поддържат Система за управление сигурността на информацията. Сигурността на информацията (стандарт ISO/IEC 27001) се отнася главно за информацията определена като актив, независимо от формата на съществуване - в електронен, хартиен или всякакъв друг формат. Т.е. Сигурността на информацията е термин различен от киберсигурността. Предвид фактът, че посочените организационни мерки в чл.3, ал.4 съдържат само част от изискуемите по стандарт мерки за сигурност на информацията и се отнасят само за киберсигурност, предлагам вместо Система за сигурност на информацията да се използват думите “Политика за киберсигурност; - Недостатъчно ясни и разбираеми текстовете относно извършването на проверки и осъществяването на контрол (виж чл.12, т.6 и	**Приема се.** **Приема се.** **Приема се.**	

	чл.27е, ал.1, т.1). От тези текстове се разбира, че министърът на електронното управление ще осъществява контрол, Националният компетентен орган към него ще осъществяват контрол. Но трябва да се отчете факта, че проверката е една от формите и методите за осъществяването на контрол. Предлагам внимателно да се прецизират текстовете отнасящи се до изършването на проверки и осъществяването на контрол; - Част от текстове са копирани директно от ДМИС2 и не са адаптирани за целите на Проекта на ЗИД на ЗКС. В чл.27л, например е посочено – Органите по чл.16 информират съответните компетентни органи съгласно Директива(ЕС) 2022/2557. Срокът за транспониране на тази Директива е 17 октомври 2024 г. и би следвало да има яснота за това кои са компетентните органи. Аналогично стои и ситуацията с национални компетентни органи по Регламент 2022/2254 там също следва да се посочи този орган в България. Предлагам в Проекта да се посочат тези органи; -Текстовете за киберкризи по чл.17а, са без конкретика – като типове киберкризи (съобразно техния обхват), управляващи кризата за всеки тип и т.н. Националната рамка за управление на киберкризи следва да регламентира дейностите при киберкризи на всички нива, включително за отделен субект, за даден сектор. В Проекта на ЗИД на ЗКС е посочен Съвета по киберсигурността (който е консултативен и координиращ орган към Министерския съвет) за компетентен орган, отговарящ за управлението на мащабните	**Приема се.** **Не се приема.**	

	киберинциденти и кризи (органи за управление на киберкризи). Считам, че Съвет имащ консултативен характер не следва да има управленски функции. -Предлагам да се определи друга структура, която има управляващи функции ца орган по управление на киберкризи; -Чл.20, ал.5 посочва международно сътрудничество посочено само в ДМИС 2. Не са посочени важни сътрудничества с МСД (Международен съюз по далекосъобщения), Организацията за сигурност и сътрудничество в Европа и др. Ако текстът се отнася за сътрудничество в сферата на киберсигурността, то следва да се допълни и за сътрудничество в киберпрестъпността, киберотбраната и кибердипломацията;. Проектът на ЗИД на ЗКС в по-голямата си част следва логиката на ДМИС 2; Предлагам да се преосмисли и да следва логиката за подредба в съответствие с националните ни особености; Считам за необходимо след чл.15, да се въведе нов член 15а, който да регламентира на кратко отговорностите и задълженията на АО по чл.16, към които се създават национални компетентни органи **НЯКОИ ДРУГИ БЕЛЕЖКИ** Чл.21, ал.1 - Публичната администрация е част от съществените субекти и нямат управителни органи. Предлагам преди думите „Управителните органи“ да се добавят думите „Административните органи и“.	**Не се приема.** **Не се приема.** **Приема се.**	Има институционална конкретика, в разпределение на роли и финкции в работата на Междуведомствена оперативна група за реакция при значителни киберинциденти, която има рзписани процедури за ескалация и управление на кризите, както и надлежна процедура за вклкючване на политическо ниво за реакция в лицето на Съвета за киберсигурност и международната организация на Европейско ниво IPCR и BluePrint. Формите на сътрудничество могат да бъдат разнородни, в зависимост от конкретния случай, не е необходимо всички форми да бъдат изчерпателно изброени в ЗКС.

	-Чл. 27ж, ал.1, т.2 предвижда органите по чл.27 е (включва и националните компетентни органи) „да извършват редовни и целеви одити на сигурността, извършвани от независим орган или компетентен орган“. Текстът в този си вид е неразбираем. Одит се извършва за установяване на съответствие на състоянието на киберсигурността с изискванията за киберсигурност (ако идеята е да се одитира сигурността на информацията, по-горе съм дал съображения, защо това е неприемливо). Трябва да се посочат изискванията в кой регламентиращ документ се има предвид. Редовните одити на какъв период следва да се извършват. ***С оглед на гореизложеното считам, че Проекът да ЗИД на ЗКС има съществени пороци е неприемлив за внасяне за разглеждане в Министерския съвет. Същият следва да се доразработи и актуялизира. След, което би било възможно до се дадта омпетнтни и коректни становища по него.*** Накрая предлагам да се прецени съобразността от коренна промяна на съществуващата система за киберсигурност в страната. Считам, че периода на изготвяне на ЗИД на ЗКС е особено подходящ за създаване на Държавна агенция за киберсигурност. В подкрепа на това мнение има редица аргументи, които са изложени в изготвен от името на Икономическия и социален съвет, АНАЛИЗ на Европейските изисквания за киберсигурност и перспективи за киберустойчива България.	**Не се приема.**	В разпоредбата на чл. 16 са регламентирани функциите на НКО. Правилата и регулярността на провеждане на одит се съдържа в НМИМИС.

„Верайзън България“ ЕООД чрез Георги Сулев	Общи коментари и основни послания ●1. Хармонизация и последователно прилагане:Хармонизацията е от съществено значение и трябва да бъде основна цел на прилагането на Директивата МИС 2 на всички нива -на ниво ЕС и на ниво държави-членки. Това включва съгласуваност на мерките за сигурност и изискванията за докладване. Това ще намали сложността, особено за многонационалните субекти, и ще предотврати създаването на мозайка от различаващи се или дори противоречащи си национални изисквания. Задълженията за киберсигурност трябва да бъдат рационални, за да се избегнат припокриващи се и/или противоречащи си задължения и ненужни тежести или разходи. Това може да бъде постигнато само ако при транспонирането се интегрира сложността и взаимодействието на директивата с други регулаторни рамки (напр. DORA и Директивата за устойчивостта на критичните субекти). ●2.Съответствие с разпоредбите на ЕКЕС:Доставчиците на телекомуникационни услуги са обект на регулиране на сигурността и устойчивостта от 2013 г. насам и следователно вече разполагат със значителни политики за сигурност и имат солиден опит в прилагането на изискванията относно мрежова и информационния сигурност като се имат предвид изискванията на ЕКЕС. Като се има предвид това, не следва да се очаква от задължените субекти да направят промени в съществуващите импрактики за сигурност, за да отговорят на изискванията на МИС 2, когато резултатъте същият. ●Техническите,организационните и оперативните мерки следва да бъдат хармонизирани и основани на	**Не съдържа предложения.**	

	принципи:Мерките следва да се основават на принципи, така че да се даде възможност на всеки субект да прилага подходящи мерки в зависимост от нивото на рисковете. Държавите членки следва да избягват установяването на специфични национални правила и да се стремят към хармонизация. Съгласно съображение 65от преамбюла на МИС 2, Групата за сътрудничество би могла да съпостави националните изисквания едни с други -това би могло да спомогне за осигуряване на последователност и съвместимост в целия Съюз и да намали административната тежест за субектите, извършващи дейност в няколко държави членки. Насърчаваме използването и/или позоваването на международни стандарти. Държавите-членки следва да се въздържат от определяне на използването на определени технологии.Това ще означава, че субектите могат да изберат технология, която отговаря по-добре на техните бизнес модели и системи, и ще гарантира, че разпоредбите няма да остареят, тъй като технологиите се променят и усъвършенстват. Приветстваме, изричното включване на принципа за технологична неутралност в ал. 1 на новия чл. 22 и новия чл. 26 (§ 24 от законопроекта). Предвид неговата важност в цялостния контекст на приложение на закона, предлагаме да бъде изведен като основен принцип на закона. ●3.Стандарти/сертифициране:Предвид динамичния характер на развитието на киберсигурността е необходимо стандартите и сертификатите да се разработват от глобални органи за определяне на стандарти, ръководени от индустрията, като например 3GPP. Съгласно Акта за киберсигурност на ЕС такива схеми трябваше да бъдат само		

	доброволни. МИС 2 се стреми да отмени това, като позволи схемите да станат задължителни. Считаме, че компетентните органи следва да се въздържат от определяне на използването на определени технологии, докато не се докаже, че те са подходящи в оперативно и икономическо отношение за икономическите оператори (независимо от техния размер). Предлагаме следното допълнение в новия чл. 25 (§ 24 от законопроекта) :„Националните компетентни органи могат да използват сертифицирани продукти, услуги и процедури по смисъла на предходното изречение, които са доказано подходящи в оперативно и икономическо отношение за всички съществени и важни субекти.Конкретни бележки по законопроекта и бъдещото му приложение от компетентните органи: ●4.Необходима е яснота и гъвкавост за субектите, предлагащи множество услуги в различни юрисдикции.Както е посочено в съображение 21, Комисията следва да предостави насоки за надзора на субекти със сложни бизнес модели, които могат да бъдат класифицирани едновременно като основен и важен субект. Държавите членки следва да разполагат с гъвкавост и да приемат, че такива многонационални субекти, предоставящи множество услуги, ще имат контрол на корпоративно ниво, а не на ниво конкретни услуги. Използването на критерия "основно място на стопанска дейност" следва да бъде прилагано за субектите със сложни бизнес модели и трансгранично присъствие. Основното място на стопанска дейност е това, което разполага с оперативен и управленски капацитет за	**Приема се.** **Приема се.**	

	прилагане на мерки за киберсигурност. При прилагането на директивата трябва да се избегне попадането на дъщерните дружества на общоевропейска група под отделна и едновременна юрисдикция на съответните държави членки. ●5."Управителни органи" не следва да се определят от компетентните органи и да се остави на субектите да ги определят по начин, подходящ за тяхната дейност.Бизнес моделите могат да бъдат сложни и не може да има универсален подход към управленските структури. Следва да се позволи на субектите да решат къде се намират отговорността и задълженията на управителните органи, дори това да е извън Съюза. ●6.Държавите-членки не следва да дават приоритет на услугите, предоставяни на големи корпоративни клиенти, в своите дейности по правоприлагане. В съображение 124 се посочва, че държавите членки могат да определят приоритетите си за надзор, като използват различни критерии или показатели. Силно подкрепяме идеята, че големите корпоративни клиенти имат значителнапреговорна сила и по-добро разбиране на рисковете за сигурността на техния бизнес и услугите, на които разчитат. Това се изразява в строги договорни ангажименти, включително SLA, права за одит и изисквания за документация. По този начин субектите, които предоставят услуги на тези корпоративни клиенти, вече имат допълнителен стимул да осигурят силни практики за сигурност. ●7.При определянето на мерките за сигурност трябва да се вземат предвид разходите.**В член 21, параграф 1 от МИС 2се казва, че при определянето на техническите,**	**Приема се.**	

	оперативните и организационните мерки трябва да се вземат предвид разходите за изпълнение. Това означава, че се приема, че някои решения може да са налични, но разходите да са твърде големи, за да бъдат разумни. Считаме, че този принцип следва да намери своето изрично отражение в § 24 от законопроекта, както се изисква от чл. 21(1) от МИС 2. Предлагаме второто изречение на ал. 1 на чл. 22 да се допълни както следва:“При спазване на принципа за технологична неутралност, отчитане на разходите за прилагане на мерките, съответните европейски и международни стандарти и технически спецификации, се гарантира ниво на сигурност на мрежовите и информационните системи, съответстващо на риска.”	**Приема се.**	
	●8. Докладването на значителни инциденти следва да бъде целенасочено. За да се избегне претоварването на компетентните органи с доклади, праговете за уведомяване за инциденти следва да бъдат определени на подходящи нива. Препоръчваме използването на абсолютни прагове (напр. 1 милион засегнати потребители) вместо качествени критерии, тъй като те по-трудно се вграждат в автоматизираните системи за докладване и водят до свръхдокладване на несъществени инциденти. Предлагаме използването на преимуществено количествени критерии за дефиниранена значителни инциденти(което е изрично предвидено и в съображение 101 от преамбюла на МИС 2) да бъде предвидено в § 24 от законопроекта. Новият чл. 24 следва да уточни, че определянето на **инцидент за значителен се осъществява чрез количествени критерии като например продължителност на инцидента и брой ползватели,**	**Приема се.**	

	засегнати от инцидента. ●9. От доставчиците, които обслужват само бизнес клиенти, не следва да се изисква да уведомяват обществеността за заплахи или киберинциденти, тъй като те нямат пряка връзка с потребителите. ●10.Предлагаме да се въведе **обслужване на едно гише** за инциденти със сигурността, съгласно различните закони.За да се намали тежестта върху субектите и да се повиши ефективността на компетентните органи, докладването на инциденти по различни режими следва да бъде централизирано -например докладването съгласно GDPR, МИС 2, Директива за e-privacy, Директивата за устойчивостта на критичните субекти. ●11.Трансграничният надзор и правоприлагането следва да се осъществяват само при ограничени обстоятелства.Член 37 от МИС 2 позволява на компетентните органи да си сътрудничат и да изискват извършването на надзорни или правоприлагащи действия по искане на друга държава членка. За да се избегне дублиране и увеличаване на тежестта върху субектите, извършващи трансгранична дейност, такива действия следва да се изискват само при ясно доказана необходимост и когато информацията не може да бъде получена чрез осъществяваната надзорна дейност на компетентния орган. ●12.Веригите за доставки се различават значително и поради това управлението на риска във веригата за доставки следва да бъде оставено на субектите, които да го определят в зависимост от своя рисков и бизнес профил.Гъвкавостта на субектите да подхождат към сигурността на веригата на доставки с подход към регулирането, ориентиран към	**Не се приема.** **Не се приема.** **Приема се.** **Не се приема.**	Директивата иизисква засегнатите субекти да бъдат уведомявани, при необходимост в случай на значителни инциденти. Предложението би довело до концептуална промяна на структурата и моделът на управление на киберигурността. Основен принцип в изграждане системата на киберсигурност, включително управление на риска във веригата за доставки е на ръководителя на субекта.

	резултатите, ще позволи да се избегне обременителната работа по договорите. С уважение, Георги Сулев		
„ЦЕТИН България“ ЕАД (ЦЕТИН)	1. Да бъде създадена нова ал. 3 на чл. 3 със следното съдържание(§ 3от ЗИДЗКС):„(3) Мерките за постигане на високо общо ниво на киберсигурност за субектите по чл. 4, т. 3, буква „а“ се определят в правилата за минималните изисквания за сигурност на обществените електронни съобщителни мрежи и услуги и методи за управление на риска за тяхната сигурностпо чл. 243, ал. 3 от Закона за електронните съобщения.“Допълнително, във връзка с горепосоченото ни предложение (тук, макар и несистематично от гл. т. структурата на ЗИДЗКС, но с цел яснота и проследимост), предлагаме в § 42 от Законопроекта:Точки 3 и 4 буква „а“ да отпаднат от ЗИДЗКС;Точка 4, буква „б“ да се измени както следва:„б) чл. 243б, чл. 243в, чл. 244 и чл. 244а се отменят“ Алтернативно, в случай че не приемете горепосоченото ни предложение, предлагаме да бъде създадена нова ал. 3 на чл. 3 със следното съдържание(за улеснение предоставяме в “bold” различната част на предложения нормативен текст):„(3) Мерките за постигане на високо общо ниво на киберсигурност за субектите по чл. 4, т. 3, буква „а“ се определят в правилата за минималните изисквания за сигурност на обществените електронни съобщителни мрежи и услуги и методи за управление на риска за тяхната сигурност, **приети от Комисията за регулиране на съобщенията. Правилата се приемат след провеждане на обществено обсъждане и се обнародват в „Държавен вестник“. При изготвянето и приемането на правилата**	**Приема се.**	

	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(ENISA), както и приложимите европейски схеми за сертифициране на киберсигурността, установени с актове на Европейската комисия, и приложимите европейски и международни стандарти и стандартизационни документи. "Останалите алинеи на чл. 3 да се преномерират съответно, независимо от това дали ще приемете основното или алтернативното ни предложение. Мотиви: На първо място,бихме искали да обърнем внимание, че настоящият ЗИДЗКС не отчита материалния напредък на доставчиците на обществени електронни съобщителни мрежи и услуги в сферата на киберсигурността, реализиран въз основа на съществуващото законодателство. Нещо повече, в него задължението за държавите членки, предвидено в чл. 21, ал. 2 от Директивата, да приемат по отношение на съществените и важни субекти(каквито са доставчиците на обществени електронни съобщителни мрежи и услуги)подходящи и пропорционални технически и организационни мерки за		

	управление на рисковете за сигурността на мрежовите и информационни системи, изобщо липсва.В чл. 3, ал. 1 от Законопроекта е предвидено, че мерките за постигане на високо общо ниво на киберсигурност се определят с наредба, издадена от Министерски съвет по предложение на министъра на електронното управление. От съдържанието на наредбата като задължени лица са изключени субектите по „чл. 4, ал. 1, т. 3, буква „а“. Независимо, че ал. 1 изобщо липсва в чл. 4 от Проекта(разпоредбата има само точки, но не и алинеи), считаме че разпоредбата цели да изключи именно „доставчицитена обществени електронни съобщителни мрежи или на обществено достъпни електронни съобщителни услуги, които отговарят на критериите за средни предприятия по смисъла на чл. 3, ал. 1 от Закона за малките и средните предприятия“ и, които са посочениv чл. 4, т. 3, б. „а“ от Проекта. Липсата в Законопроекта на изрична законова делегация за приемане на такива правила за доставчиците на обществени електронни съобщителни мрежи или услуги, считаме засъществена празнина(или по-скоро нормативен пропуск при изготвянето на Законопроекта), която поставя в неяснота и дори изцяло изключва мерки, които следва да се приемат и прилагат спрямо последните. Съображение 95 от МИС2 допълнително предвижда, че „когато е целесъобразно и за да се избегнат ненужни смущения, съществуващите национални насоки, приети за транспониране на правилата, свързани с мерките за		

	сигурност по членове 40 и 41 от Директива (ЕС) 2018/1972, следва да се вземат предвид при транспонирането на настоящата директива, като по този начин се надгражда върху вече придобитите знания и умения съгласно Директива (ЕС) 2018/1972 относно мерките за сигурност и уведомленията за инциденти.“Приетите от КРС на основание чл. 243, ал. 3, изр. първо от Закона за електронните съобщения (ЗЕС)Правила за минималните изисквания за сигурност на обществените електронни съобщителни мрежи и услуги и методи за управление на риска за тяхната сигурност (Обн., ДВ, бр. 42 от 07.06.2022 г.(Правилата) следва да бъдат запазени, като при необходимост бъдат изменени и допълнени с цел пълно съответствие с Директивата.Макар и приети с подзаконов акт по ЗЕС при транспонирането на чл. 40 и 41 от Директива (ЕС) 2018/1972 Правилата на КРС адекватно отчитат основните положения на МИС2. Самите Правила бяха приети през 2022 година, като отмениха Раздел II и приложение No 1 към чл. 8, ал. 2 от Общите изисквания при осъществяване на обществени електронни съобщения. С цел яснота и регулаторна предвидимост, а и за да се избегне уреждането на някои от въпросите (напр. докладването на инциденти) в трети пореден нормативен акт за последните 3 години, считаме че изискванията на Директиватаследва да бъдат въведени именно в посочените Правила. Противното би създало допълнителна административна тежестза предприятията, предоставящи обществени електронни съобщителни мрежи и услуги, които вече ефективно ЗОрепизпълняватизискванията на Правилата на КРС, вкл. детайлните технически и организационни мерки за		

	сигурност (Приложение No 1 към Правилата), които включват цели 8 отделни области на сигурност, респ. значителните 29 различни цели на сигурност.Предложението ни е съобразено с изискването за „равностоен ефект“на задълженията, предвидено в чл. 4, пар. 2, б. „а“ и „б“от МИС2, като допълнително отчита и Насоките на Комисията относно прилагането на чл. 4, параграфи 1 и 2 от Директивата, в т. II.1.6, от които е изрично е посочено, че ако специфичните секторни изисквания са подробни или по-детайлни от тези по МИС2, трябва да се прилагат последните.Не на последно място, настоящото ни предложение отчита и факта, че Законопроектът определя КРС като Национален компетентен орган (НКО) за доставчиците на електронни съобщителни мрежи и електронни съобщителни услуги. По тази причина, уместно и напълно логично е Правилата да запазят своята приложимост и при транспонирането на МИС2 в националното законодателство. 2.Алинея 7 на чл. 15 да отпадне(§ 16, т.4 от ЗИДЗКС). Мотиви: Предвиденият в ал. 7 автоматизиран обмен на данни между информационните системи за сигурност на стратегическите обекти и дейности и Центъра на ДАНС за мониторинг и реакция на инциденти със значително увреждащо въздействие върху комуникационните и информационните системи на стратегическите обекти и	**Не се приема.**	Чрез ЗИД на ЗКС се обективира работата на Център за мониторинг и реакция на инциденти със значително увреждащо въздействие върху комуникационните и информационните системи на стратегическите обекти и дейности, които са от

	дейности, които са от значение за националната сигурност,не съответства на Съображение 24 от МИС 2. В посоченото съображение изрично е предвидено, че механизъм за автоматично и пряко докладване следва да бъде въведен на национално само когато това е целесъобразно, но дори и в тези случаи посоченият механизъм може да бъде предназначен за систематичен и незабавен обмен на информация само с ЕРИКС, компетентните органи или единните звена за контактотносно разглеждането на такива уведомления за инциденти.С други думи, в Директивата няма предвидено правно основание за въвеждане на подобен механизъм за автоматизиран обмен с органите в областта на националната сигурност. В допълнение следва да се посочат и чл. 2, пар. 6 и 7 от МИС 2, както и самиятЗИДЗКС, който в чл. 7, т. 3предвижда, че „този закон не се прилага... по отношение на информационните системи, дефинирани като критични в стратегически обекти или субектите, осъществяващи стратегически дейности, определени от ръководителите на стратегическите обекти и възлагащите стратегически дейности, които са от значение за националната сигурност, по смисъла на Наредбата за условията и реда за определяне на мерките за защита на информационните и комуникационните системи на стратегическите обекти от значение за националната сигурност и за осъществяването на контрол“. Тоест в самия Законопроект е въведено изрично нормативно изключениев тази посока.	**Приема се.**	значение за националната сигурност, която предвижда автоматизиран обмен на информация между ръководителите на стратегически обекти и възлагащите и извършващите стратегически дейности от значение за националната сигурност с Центъра. С развитието на технологията се увеличава процесът на автоматизация и споделяне на информация за инциденти.

	3.Член 23 да отпадне(§ 24от ЗИДЗКС) Мотиви: Предвидените нови законови правомощия на Съвета по киберсигурностда идентифицира и прави оценка на технологичните и нетехнологичните рискове, като изготвя съгласувано с компетентните органи мотивирано предложение до МС да ограничи използването на конкретни технологии или на критични вериги за доставка на ИКТ услуги, ИКТ системи или ИКТ продуктови вериги за доставка, респ. на МС да се произнася с административен акт, издаден по реда на АПК, генерално не съответстват на Директивата. Посочената разпоредба не може да бъде приета като национална мярка, надхвърляща мерките по самата МИС 2, тъй като de factoпредставлява резултат от смесването на два различни правопорядъка –Общностния и националния посредством въвеждането на правомощия на национален орган (Съветът по киберсигурност), които не са предвидени в самата Директива. Последното не се променя от въведеното в Законопроекта условие „доколкото с това не се засягат императивни разпоредби на правото на Европейския съюз или на действащото българско законодателство“, които са общи и бланкетни, респ. да „не се влиза в противоречие с		

	координираните оценки на риска на ниво Европейски съюз“. По отношение на последното, допълнително посочваме, че видно от самото заглавие на чл. 22 от МИС2, посочената оценка се прави на равнище ЕС –Член 22 „Координирана на равнището на Съюза оценка на риска за сигурността на критични вериги за доставка“. Съгласно чл. 22, пар. 1 от Директивата посочените оценки на риска за сигурността на конкретни критични вериги за доставка на ИКТ услуги, ИКТ системи или ИКТ продуктови вериги за доставка могат да се правят от Групата за сътрудничество, заеднос Комисията и ENISA(чл. 22, пар. 4Open2 от Директивата),а не от национални органи, какъвто е МС.Нещо повече, на МС не са предоставени правомощия с действащото законодателство в тази връзка, с оглед на което и разпоредбата на чл. 23 в частта и „в рамките на предоставените му с действащото законодателство правомощия“препраща на практика към несъществуваща нормативна база. С други думи, със ЗИДЗКС е направено своеобразно дописване на Директива (ЕС) 2022/2555, посредством въвеждането на непредвидени в самата Директива неясни и с липсваща нормативна рамка национални механизми за имплементиране на координирани на оценки на риска, които по Директива са предвидени не на национално, а на равнище на Съюза.Не на последно по важност мястои в контекста на предвиденото по-горе, в новия чл. 23 не са предвидени абсолютно никакви гаранции за адекватна		

	защита на правата и интересите на съществените и важни субекти по чл. 4а от Законопроекта, вкл. посредством съгласуването с последните на подобни административни мерки, доколкото такива мерки (общо и неопределено наречени „административен акт“в Проекта) са въобще допустими с оглед изискванията на самата Директива (ЕС) 2022/2555. 4.В чл. 25 „НКО“ да бъде заменено със„Съвета по киберсигурност“, съответно(и с цел систематичност), да бъде създадена нова т. 8 на чл. 10, с която на Съвета по киберсигурност да бъде възложено предвиденото ново законово правомощие(§ 24 от ЗИДЗКС).Алтернативно, това правомощие да се възложи директно на Министерски съвет. Мотиви: Предвиденото законово правомощие за изискване с цел доказване на съответствието с конкретни изисквания по чл. 22 от съществените и важните субекти да използват конкретни ИКТ продукти, ИКТ услуги и ИКТ процедури, които са разработени от тях или са придобити от трети страни, сертифицирани в рамките на европейските схеми за киберсигурност, приети съгласно член 49 от Регламент (ЕС) 2019/881 е съществено и следва да се упражнява не от НКО, а на по-високо и централно ниво–	**Не се приема.**	Съветът по киберсигурността е консултативен орган, НКО за съответния сектор познава в детайли дейността на сектора и на оперативно ниво, поради което считаме, че е по-целесъобразно той да изиска от съществените и важните субекти да използват конкретни, доказано подходящи в оперативно и икономическо отношение ИКТ продукти, ИКТ услуги и ИКТ процедури, които са разработени от тях или са придобити от трети страни, сертифицирани в рамките на европейските схеми за киберсигурност, приети съгласно член 49 от Регламент (ЕС) 2019/881 на Европейския парламент и на Съвета от 17 април 2019 година относно ENISA (Агенцията на Европейския съюз за киберсигурност) и сертифицирането на киберсигурността на информационните и комуникационните технологии, както и за отмяна на Регламент (ЕС) № 526/2013 (Акт за киберсигурността) (ОВ, L 151 от 7 юни 2019 г.).

	от Съвета по киберсигурносттакато консултативен и координиращ орган към Министерски съвет (МС) по въпросите на киберсигурността(чл. 9 от ЗКС)или от самия МС.Предложената промяна не само е в съответствие с чл. 24 от Директивата, като допълнително представлява логично и нормативно продължение на чл. 10 от ЗКС, предвиждащ редица съществени законови правомощия именно на Съвета по киберсигурност, като например: предлагане на МС Национална стратегия за киберсигурност и пътната карта към нея (т. 2); даване предложения за хармонизиране и координиране на секторните политики за постигане на високо общо ниво на киберсигурност на икономиката и обществото (т. 5); предлаганена Национален план за реакция при мащабни киберинциденти и кризи (т. 6) и т.н.Предоставянето на това правомощие на централизиран национален орган ще осигури систематично и последователно прилагане на тази мярка на национално ниво за всички сектори и ще ограничи прилагането на различен подход от страна на различните НКО, които се създават към административните органи, определени с решение на МС. 5.В чл. 29, ал. 3, 4 и 6 да бъдат премахнати долните граници на предвидените нови имуществени санкциизасъществените и важните субекти, респ. за управителите или членовете на управителните им органи(§ 29от ЗИДЗКС). Мотиви: Предвидената минимални имуществени санкции (от 200 000 лв.!за съществените субекти,	**Приема се частично.**	В ЗИД на ЗКС са намлени размирите на предвидените санкции, включително и минималните им размери.

	например) са прекомерни и необосновании по никакъв начин не отговарят на изискванията на МИС 2 (чл. 34, пар. 1), а и на самия ЗИДЗКС (чл. 29, ал. 1) да бъдат „ефективни, пропорционални и възпиращи“Подобни прекомерни санкции допълнително: драстично ограничават оперативната самостоятелност на административните органи по чл. 16, ал. 1от ЗИДЗКС като административнонаказващи органи; представляват механично намаление на минималния размер на максималния праг по МИС 2; необосновано се прилагат генерално за всякакви видове потенциални нарушения на задълженията по чл. 22 и чл. 24 от Законопроекта, които в редица случаи биха били, ако не малозначителни, то с изключително ниска степен на обществена опасност, която по никакъв начин не оправдава налагането на имуществена санкция от минимум 200 000 лв.5Open6.В § 42 от ПЗР по отношение на ЗЕС да бъдат направени следните изменения и допълнения(в допълнение към предложените в т. 1 от настоящото становище, които също касаят § 42, но сме дали по-горе с цел яснота и проследимост, тъй като са пряко свързани с чл. 3 на Законопроекта):6.1.Точка 1 да придобие следната редакция:„1. В чл. 30, ал. 1 от Закона за електронните съобщения се създава нова т. 30 със следното съдържание:30. изпълнява функциите на национален компетентен орган по чл. 16, ал. 3 от Закона за киберсигурността по отношение на субектите по	**Приема се.**	

	чл. 4, т. 3, буква а) и б) от Закона за киберсигурността“ Мотиви:Предложението отчита Съображение 95 от Преамбюла на Директивата предвижда, че „държавитечленки могат да възложат ролята на компетентни органи в областта на електронните съобщения на националните регулаторни органи съгласно Директива (ЕС) 2018/1972, за да се гарантира продължаването на действащите практики и да се надгражда върху знанията и опита, придобити в резултат на прилагането на посочената директива“.Предложението допълнително създава условия за плавен преход към предстоящото прилагане във вътрешен аспект на квалифицираните изисквания и механизми на МИС2 от компетентния и разполагащ с необходимата експертиза национален регулаторен орган –секторния регулатор КРС и неговото дългогодишно сътрудничество с ENISA, вкл. специфични знанияи опит в прилагането на Регулаторната рамка, Директива (ЕС) 2018/1972за установяване на Европейски кодекс за електронни съобщения, и националните закони, които ги транспонират –ЗЕС, ЗЕСМФИ и подзаконовите актове по тяхното прилагане.Горепосочените мотиви на пръв поглед са отчетени на Законопроекта, но същевременно с това, в § 42 от ПЗР на ЗИДЗКС са налице редица несъответствия: препращане към несъществуваща ал. 1 на Законопроекта(чл. 4 няма алинеи, а само точки); липса на уточнение, че всъщност става дума за референция именно към чл. 4 от ЗКС, а не към ЗЕС, тъй като чл. 4 на ЗЕС, към който се препраща, се отнася до целите на ЗЕС, а не до		

	компетентните органи; сгрешено посочване на чл. 16, който по ЗКС действително касае НКО, но по ЗЕС, който е предмет на ПЗР-то, в същия като номерация член са регламентирани правомощията на министъра на транспорта и съобщенията, а не на КРС. Самото ни предложение за създаването на нова т. 30 на чл. 30, ал. 1 от ЗЕС отчита систематично място на компетенциите на КРС, чиито законови правомощия са изброени именно чл. 30 от ЗЕС. 6.2.Да бъде създаден нов чл. 39а със следното съдържание: „Чл. 39а. Комисията създава секторен екип за реагиране при инциденти с компютърната сигурност (СЕРИКС) по чл. 18, ал. 1 от Закона за киберсигурността“. Екипът се създава към Комисията в съответствие с методическите указания на Агенцията на Европейския съюзза киберсигурност (ENISA).“ Мотиви: Съгласно чл. 16, ал. 1 от ЗИДЗКС МС определя с решение административните органи, към които се създават национални компетентни органи по киберсигурност (НКО), когато такива не са създадени със специален закон. В тази връзка, разпоредбата на чл. 18, ал. 1 от Законопроекта предвижда, че посочените административните органи създават секторни екипи за	**Не се приема.**	Задълженията на НКО са уредени в ЗКС.

	реагиране при инциденти с компютърната сигурност (СЕРИКС).КРС попада в предвиденото изключение по чл. 16, ал. 1 от ЗИДЗКС, тъй като със специален закон (§ 42 от ПЗР на ЗИДЗКС, а именно специалния ЗЕС) Комисията директно е определена за НКО. С други думи, КРС de factoce явява едновременно както административен орган по чл. 16, ал. 1, така и НКОпо същата разпоредба, без обаче първото (административен орган) да е изрично посочено в Законопроекта –§ 42 от ПЗР говори само за НКО. Същевременно обаче, на основание чл. 18, ал. 1 от ЗИДЗКС именно административните органи, а не НКО към тях, определят съответния СЕРИКС. Предвид гореизложеното и цел яснота, вкл. от институционална гл. т., предлагаме създаването на новия чл. 39а на ЗЕС. 6.3.Да бъде предвиден преходен период до влизането в сила на новите, съответно ревизирани спрямо МИС 2, правила на КРС по чл. 3, ал. 3 от ЗКС, в който действащите Правила 6Opeпза минималните изисквания за сигурност на обществените електронни съобщителни мрежи и услуги и методи за управление на риска за тяхната сигурност (Обн., ДВ, бр. 42 от 07.06.2022 г. да запазят своето правно действие. Мотиви:Реферираме към мотивите ни по т. 1 от настоящото становище. Допълнително посочваме, че предвижданeто на такъв преходен период е необходимо както с оглед горепосоченото съображение 95 от МИС 2, така и с цел	**Приема се.**	

	избягването на правен и регулаторен вакуум до съответното изменение и допълнение на Правилата с цел пълно съответствие с Директива (ЕС) 2022/2555.		
	7.В допълнение на изложеното бихме искали да подчертаем, че Проектът има нужда от цялостен и внимателен прочит и ревизия на всички препратки към разпоредби от същия закон, както и от други закони, специално тези към ЗЕС. В тази връзка посочваме примерно inter aliaследните неточни препратки,без да претендираме за изчерпателност: -Всички препратки към чл. 4 със съответни алинеи –чл. 4, ал. 1, чл. 4, ал. 2 и т.н. от ЗКС(като напр. тази в чл. 3, ал. 2, в чл. 4а, ал. 1, т. 3 –6 и т.н.) следва да бъдат към чл. 4 от ЗКС със съответни точки, тъй като в последния няма алинеи, а само точки, както сме посочили по-горе.	**Приема се.**	
	-Препратката в чл. 17, ал. 9 от ЗКС към чл. 16, ал. 3, т. 5 от закона също не е коректна, доколкото предмет на въпросната разпоредба не са секторните компетентни органи, а стандарти, по които НКО изготвят препоръки-Всички препратки към чл. 16, ал. 1 визират единствено и само НКО,определени с решение на МС, а КРС е национален компетентен орган, създаден със самия закон, който следва да се третира равнопоставено с всички останали НКО, респективно всички препратки следва да се тълкуват направени и приложими не само за НКО по чл. 16, ал. 1, но и за КРС като такъв по силата на изричната разпоредба на § 42, т. 1 от Законопроекта (напр. чл. 18, ал. 1 и сл.).	**Приема се.**	

	8.Прави впечатление също, че законовите дефиниции са непоследователни и могат да създадат сериозни затруднения в правилното тълкуване на Законопроекта и прилагането му след като бъде приет и влезе в сила. В това отношение като пример може да бъде посочената дефиницията за „административен орган “. За целите на дефиниране на „административен оран “Законопроектът препраща към § 1, т. 1 от Административнопроцесуалния кодекс, според който А дминистративен орган е „органът, който принадлежи към системата на изпълнителната власт, както и всеки носител на административни правомощия, овластен въз основа на закон включително лицата, осъществяващи публични функции, и организациите, предоставящи обществени услуги“.По този начин дефиницията за административен орган обхваща, освен друго,и предприятията, предоставящи обществени услуги,в това число предприятията,предоставящи обществени електронни съобщителни услуги. В резултат на товаможе да се счете, че НКО по отношение на предприятията, предоставящи електронни съобщителни услуги, съгласно чл. 16, ал. 2 от Законопроекта е Министерството на електронното управление, а не КРС, респ. да създаде колизиция между разпоредбите на чл. 16, ал. 2 от Законопроекта и разпоредбата на § 42, т. 1 от Преходните и заключителните му разпоредби, с която се изменя чл. 16 ЗЕС като се създава нова ал. 2а в същия В тази връзка считаме за наложително ревизията на дефинициите на Законопроекта в контекста на внимателен прочит на съществуващите дефиниции на действащите нормативни актове. Оставаме на Ваше разположение, в случай че имате	**Приема се.**	

	допълнителни въпроси.		