Фондация „Право и Интернет“
гр. София, ул. „Българска морава” № 54, ет.7
тел.: + 359 2 44 606 44 факс: + 359 2 44 606 46
e-mail: office@netlaw.bg, **www.netlaw.bg**

Изх. № 2129/01.08.2024

ДО
МИНИСТЕРСТВО НА ЕЛЕКТРОННОТО УПРАВЛЕНИЕ

Г-Н ВАЛЕНТИН МУНДРОВ – Министър на електронното управление
Mail@egov.government.bg

Г-ЖА БИСЕРКА РАДЕВА – Директор на дирекция „Мрежова и информационна сигурност“
b.radeva@egov.government.bg

Уважаеми г-н Министър,
Уважаема г-жо Радева,
Уважаеми дами и господа,

В качеството си на неправителствена организация, която се занимава активно в областта на правните, технологичните, икономическите и социалните въпроси, свързани с бързото навлизане на информационните и комуникационни технологии както в публичния, така и в частния сектор, с настоящото представяме нашата позиция относно публикувания проект на Закон за изменение и допълнение на Закона за киберсигурност, с който се предвижда транспониране на Директива (ЕС) 2022/2555 (Директива МИС 2)[1].

В контекста на стремителното развитие на технологиите и влиянието им върху ежедневието на гражданите и обществото, и предвид наблюдаваното увеличаване на заплахите за и пробивите в мрежите и информационните системи, своевременното актуализиране на законодателната рамка, регулираща тези отношения, е наистина наложително.

Позицията е изготвена от експертите на Фондация „Право и интернет“, които имат задълбочен и дългогодишен опит в сферата на електронните съобщения, информационните и комуникационни технологии, и конкретно в сферата на сигурността на мрежите и информационните системи/киберсигурността. Документът съдържа по-общи предложения и препоръки за усъвършенстване на законопроекта, както и някои по-конкретни насоки и добри практики, които да послужат за провеждането на задълбочен и конструктивен диалог в хода на законодателната процедура по приемането на този изключително важен за държавата и обществото инструмент.

Приложение: Становище относно проект на Закон за изменение и допълнение на Закона за киберсигурност

Фондация „Право и интернет“

Проф. д-р Даниела Илиева

[1] *https://www.strategy.bg/PublicConsultations/View.aspx?lang=bg-BG&Id=8439*

СТАНОВИЩЕ ОТНОСНО ПРОЕКТ НА ЗАКОН ЗА ИЗМЕНЕНИЕ И ДОПЪЛНЕНИЕ НА ЗАКОНА ЗА КИБЕРСИГУРНОСТ

С оглед наближаващия краен срок за транспониране в националното законодателство 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 (долу „Директивата“) следва да се приветства публикуваният проект на Закон за изменение и допълнение на Закона за киберсигурност (ЗК), с който се предвижда транспониране на Директива МИС 2 (долу „ЗИД“ или законопроектът).

Законопроектът поставя изключително добра основа за последващите стъпки по приемането на ЗИД в Народното събрание, поради което с настоящото искаме да обърнем внимание на няколко аспекта от законопроекта, които ни направиха впечатление и които биха могли да се подобрят и претърпят редакции с оглед задълбочаване на диалога за усъвършенстване на предложения законодателен акт.

<u>В обобщен вид коментарите и предложенията ни засягат следните въпроси:</u>

1. Предложения за техническа редакция на чл. 3, ал. 2 ЗК, изясняване на приложимите мерки за предприятията, предоставящи електронни съобщителни мрежи или услуги и уточняване на органа, който следва да ги приеме.

2. Предложения за редакция на дефинициите за административни органи, организациите за обществени услуги и лицата, изпълняващи обществени функции, за да се избегне прекалено широк обхват на закона, както и уточняване на обхвата на образователните институции, поради наличието на конфликт между различните дефиниции в закона.

3. Предложение за допълнение на новия чл. 22 ЗК за постигане на по-голямо съответствие с Директивата (като се включи изричен текст, че мерките се прилагат при отчитане на разходите за прилагането им и предвид последните постижения в областта).

4. Предложения за промени относно това кои субекти се считат за съществени и важни, за да се постигне последователното прилагане на закона и баланс с Директивата, както и за въвеждане на правила относно отпадането на приложимостта на мерките по отношение на лица, които вече не отговарят на критериите за съществен или важен субект (вкл. за заличаване от регистъра).

5. Предложение за допълнение на новия чл. 23, за да се постигне по-голяма консистентност с чл. 22 от Директивата.

6. Препоръки относно намаляване на минималния размер на санкциите и по-ясни правила за извънплановите проверки за намаляване на административната тежест и яснота за субектите.

7. Предложение за установяване на преходен период за налагане на санкции с оглед множеството нови правила, очаквани подзаконови нормативни актове и увеличението на санкциите.

8. Предложения за технически корекции и допълнения на дефинициите.

Конкретните ни коментари и препоръки са следните:

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 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.

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 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 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.

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 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 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 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.

<u>В заключение, предложението ни е за:</u>

- 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).

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.

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.

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.

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 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.

1.7. Като се има предвид чл. 2, параграф 7 от Директивата [2]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.

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.

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 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 тежест 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.

[2] *7. Настоящата директива не се прилага за органи на публичната администрация, които извършват дейности в областта на националната сигурност, обществената сигурност, отбраната или правоприлагането, включително предотвратяването, разследването, разкриването и наказателното преследване на престъпления.*

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.

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.

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 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

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, 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.

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“ 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.

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 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.

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 силно препоръчително да има преходен период след определянето им съгласно §41 за субектите, в който да могат да изпълнят всички задължения по закона.

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.

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 на

електронното 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 редакция в §41 ЗИД, за да се прецизира текстът и поясни, че субектите се определят от националните компетентни органи.

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.“

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.

1.19. Няколко допълнителни предложения:

- Препоръчително е да се предвидят ясни и прозрачни процедури и правила, при които 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.

- 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.

- 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 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

- 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-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.

DANIELA NIKOLAEVA ILIEVA
Digitally Signed with a Qualified E-Signature. Qualified Time-stamped. Date: 01.08.2024 13:28:32 Z Compliant with eIDAS.