НАРОДНО СЪБРАНИЕ
Вх.No 51-554-04-140
Дата 20 / 03 2025

12
16

ЧРЕЗ ПРЕДСЕДАТЕЛЯ НА
51-ОТО НАРОДНО СЪБРАНИЕ

ДО
ПРЕДСЕДАТЕЛЯ НА
КОМИСИЯТА ПО ЕЛЕКТРОННО
УПРАВЛЕНИЕ И
ИНФОРМАЦИОННИ ТЕХНОЛОГИИ
Г-Н ЛЕВЕНТ МЕМИШ

УВАЖАЕМИ Г-Н ПРЕДСЕДАТЕЛ,

На основание чл. 79, ал.1 от Правилника за организацията и дейността на Народното събрание, правим следните мотивирани изменения и допълнения в Законопроекта за изменение и допълнение на Закона за киберсигурност (51-402-01-17) ОТ 12.12.2024г.:

1. В § 3, чл.3,т. 4 , ал. 3 думите "по предложение на Комисията за регулиране на съобщенията и на министъра на електронното управление" се заменят с думите "**по предложение на министъра на електронното управление"**
Мотиви: КРС е регулатор и не може да се меси в работата на МЕУ, както и да предлага наредби. Тяхната функция е да регулрат сектора, а не да пишат наредби.

2. В § 6 чл.5, т. 2 Предложението в "т. 2 думите „Служба „Военно разузнаване" се заменят с „Комисията за противодействие на корупцията", предложението да отпадне.

Мотиви: В § 5, т. 2 са описани ведомствата за които не подлежат на прилагането на този закон имайки в предвид, че тези ведомства не са свързани с предоставянето на административни услуги по електронен път и обмен на електронни документи между административните органи. В тази връзка КПК предоставя административни услуги и по електронен път, както

и приема документи по електронен път и не би следвало да отговаря на изискванията на закона за киберсигурност.

3. В § 6 чл.5 т.3, предложението „точки 4 и 5 се отменят“ и се заменя с „ точка 5 се отменя“

Мотиви: В § 5, т. 3 се предлага отмяна на точка 4, която се отнася за за доставчици на удостоверителни услуги по смисъла на чл. 3, т. 19 от Регламент (ЕС) № 910/2014 г. на Европейския парламент и на Съвета от 23 юли 2014 г. относно електронната идентификация и удостоверителните услуги при електронни трансакции на вътрешния пазар и за отмяна на Директива 1999/93/ЕО (ОВ, L 257/73 от 28 август 2014 г.) , която гласи следното: *„доставчик на удостоверителни услуги“ означава физическо или юридическо лице, което предоставя една или повече удостоверителни услуги като доставчик на квалифицирани или на неквалифицирани удостоверителни услуги*;, В този смисъл и в предвид естеството на закона не намирам причина тази точка да отпадне в предвид, че ясно е описано за какво става въпрос в чл. 3, т. 19 от Регламент (ЕС) № 910/2014 г.

4. В § 10, чл. 8, ал. 2 текста се променя по следният начин:

„(2) Като част от Националната стратегия за киберсигурност министърът на електронното управление, **в координация със Съвета по киберсигурността**, провежда политиките:

Мотиви: Координацията със Съвета по киберсигурността засилва междуинституционалния подход.

5. В § 10, чл. 8, ал. 2 , т.1 текста се променя по следният начин:

1. за киберсигурността по веригата за доставки на ИКТ продукти и услуги, включително разработване на минимални изисквания за сигурност на доставчиците и ежегодна оценка на рисковете в критични вериги;

Мотиви: Уточнението за минимални изисквания и ежегодна оценка на веригите за доставки повишава сигурността в ключови сектори.

6. В § 10, чл. 8, ал. 2 , т.10 текста се променя по следният начин:

10. по насърчаване на активна киберзащита, включително чрез стимули за внедряване на системи за ранно предупреждение и автоматизирано откриване на заплахи.“

Мотиви: Задължителните изисквания при обществените поръчки и стимулите за активна защита (напр. ранно предупреждение) насърчават проактивност и иновации.

7. В § 19, чл. 17а, ал. 2 се променя по следният начин:

„(2) Съветът по ал. 1 приема национален план за реакция при мащабни киберинциденти и кризи, подлежащ на актуализация на всеки две години, в който се определят целите, условията и редът за управление на мащабни киберинциденти и кризи. Планът се разработва в сътрудничество с Националното единно звено за контакт и включва:

1.целите на националните мерки за подготвеност, базирани на анализ на риска и сценарии за кризи;

2.ясни задачи и отговорности на органите за управление на киберкризи, включително резервни механизми при недостъпност на ключови лица;

3.процедури за управление на киберкризи, интегрирани в общата рамка за управление на кризи, с приоритетни канали за обмен на информация в реално време;

4.национални мерки за подготвеност, включително задължителни ежегодни учения с участие на публичния и частния сектор;

5.списък на ключови заинтересовани страни от публичния и частния сектор, както и на критична инфраструктура, подлежаща на защита;

6.национални и трансгранични процедури за координация с европейските институции, включително симулации на съвместни действия с мрежата на ЕС за киберкризи.“

Мотиви: Актуализацията на всеки две години гарантира, че планът отговаря на новите заплахи. Сътрудничеството с Националното единно звено за контакт и уточненията за реално време и ежегодни учения повишават практическата готовност.Включването на трансгранични симулации отразява изискванията на NIS 2 за сътрудничество в ЕС.

8. В § 25 чл.21 т.2 думите „на всеки две години“ се заменят с „ на всеки 12 месеца“

Мотиви: Срока от две години е твърде голям в предвид дигиталната ера в която живеем. Когато законодателя задължи управителните органи на съществените и важните субекти и административните органи на всеки 12 месеца да преминават обучение за придобиване на познания и опресняване на знанията ще имат повече познания в управлението на риска от Кибер заплахи.

9. В §25 чл. 22 ал.2 т.3 думата „ например“ се премахва.

Мотиви: Закона има за цел да дава ясни насоки за неговото изпълнение, а не примери. Предполагам е техническа грешка.

10. В §30 чл. 29, чл.1 Глобите и имуществените санкции се налагат независимо, от която и да е от мерките, посочени в чл. 27и, ал. 1, т. 2-7 и чл. 27к. се променя по следният начин:

(2) Съществен субект, който не изпълни задълженията по чл. 22 и 23, **подлежи** на имуществена санкция между 50 000 лв. и по-високата стойност между:

А. 2 на сто от общия световен годишен оборот за предходната финансова година на предприятието, към което принадлежи важният субект

Б. Сумата от 20 милиона лева

(3) Важен субект, който не изпълни задълженията по чл. 22 и 23, подлежи на имуществена санкция между 25 000 лв. и по-високата стойност между:

А. 1,4 на сто от общия световен годишен оборот за предходната финансова година на предприятието, към което принадлежи важният субект

Б. Сумата от 14 милиона лева

Мотиви: С цел привеждане в съответствие с член 34, параграфи 4 и 5 от Директивата NIS2 препоръчваме заличаване на минималните размери на глобата от 20 млн. лв. и 14 млн. лв. в член 29, параграфи 2 и 3 от проекта на Закон за киберсигурността В чл. 34, ал. 4 и 5 от Директивата NIS2 е предвидено, че максималният размер на глобите не може да бъде по-малък от по-високата от следните стойности (i) 10 млн. евро и 2 % от общия световен годишен оборот за предходната финансова година на предприятието (за значими субекти); и (ii) 7 млн. евро и 1,4 % от общия световен годишен оборот за предходната финансова година на предприятието (за значими субекти) Това не са минималните нива на глобите, които се налагат.

11. В §25 в чл.22 точка 11 и точка 12 се премахват.

Мотиви: Проектът на Закон за киберсигурността следва да отразява предложенията на Директивата NIS2. Допълнителните политики, посочени в член 22, параграф 2, точка 11 и член 22, параграф 2, точка 12, не се съдържат в Директивата NIS2.

Добавянето им в българския закон за изпълнение би превърнало България в изключение в ЕС, когато в Директивата NIS2 се набляга на хармонизиран подход. Например, целта на Директивата NIS2 е „да се *постигне високо* ***общо ниво на*** *киберсигурност в целия Съюз с оглед подобряване на функционирането на вътрешния пазар*“1

12. В § 25, чл. 24 се променя по следният начин:

За да се докаже съответствие с изискванията по чл. 22, Националният компетентен орган (НКО), след консултация със Съвета по киберсигурността, може да препоръча на съществените и важните субекти използването на ИКТ продукти, услуги и процедури, сертифицирани по европейските схеми за

киберсигурност съгласно Регламент (ЕС) 2019/881, когато те са доказани като оперативно и икономически ефективни чрез публично достъпен анализ. Задължително използване може да се изиска само при наличие на висок риск за националната сигурност, обоснован с писмено решение.

Мотиви: Замяната на „изисква“ с „препоръчва“ и ограничаването на задължителността само при висок риск запазва технологичната неутралност и избягва ненужни разходи за субектите.

13. В §29 чл.27к, т.5 текста се променя по следният начин:

Членовете на управителните органи на съществени и важни субекти одобряват мерките за управление на риска в областта на киберсигурността, предприети от тези субекти с цел спазване на чл. 22, следят за тяхното изпълнение и носят отговорност за нарушения на този член от страна на субектите.

Мотиви: Предложението е да се приведе в съответствие с член 20, параграф 1 от Директивата за МИС2.

14. Създава се чл. 29б със следният текст:

Когато предприема някоя от мерките за изпълнение, посочени в членове 27, 28 и/или 29, компетентният орган спазва правото на защита и взема предвид обстоятелствата по всеки отделен случай и като минимум надлежно отчита:

(а) сериозността на нарушението и важността на нарушените разпоредби

(i) повторни нарушения

(ii) неуспешно уведомяване или отстраняване на значителни инциденти

(iii) неизпълнение на задължението за отстраняване на недостатъци след задължителни указания от [компетентния орган].

(iv) възпрепятстване на одити или дейности по мониторинг, разпоредени от компетентния орган след установяване на нарушение

(v) предоставяне на невярна или грубо неточна информация във връзка с мерките за управление на риска в областта на киберсигурността или задълженията за докладване, предвидени в членове 22 и 23

(б) продължителността на нарушението

(в) всички съответни предишни нарушения, извършени от съответния субект

(г) всички причинени материални или нематериални вреди, включително всякакви финансови или икономически загуби, последици за други услуги и брой на засегнатите потребители

(д) евентуални умисъл или небрежност от страна на извършителя на нарушението

(е) всички мерки, предприети от субекта за предотвратяване или намаляване на материалните или нематериалните вреди

(ж) всяко придържане към одобрени кодекси за поведение или одобрени механизми за сертифициране

(з) степента на сътрудничество на физическите или юридическите лица, привлечени към отговорност, с компетентните органи

15. В преходни и заключителни разпоредби §42 се премахва.

Мотиви: Добавянето на този параграф в българския закон за изпълнение би превърнало България в изключение в ЕС, когато в Директивата NIS2 се набляга на хармонизиран подход. Например, целта на Директивата NIS2 е „да се *постигне високо **общо ниво на** киберсигурност в целия Съюз с оглед подобряване на функционирането на вътрешния пазар*“, никъде в директивата не се споменава за създаване на център за киберсигурност в министерството на Енергетиката. Такъв център ще дублира функцията на националният център за киберсигурност.

ВНОСИТЕЛИ:

Костадин Тодоров Костадинов

Артем Николаев Славов

Никола Ангелов Димитров

Виолета Радева Карпачева