

РЕПУБЛИКА БЪЛГАРИЯ
ЧЕТИРИДЕСЕТ И ОСМО НАРОДНО СЪБРАНИЕ

КОМИСИЯ ПО ВЪПРОСИТЕ НА ЕВРОПЕЙСКИЯ СЪЮЗ

ДОКЛАД

ОТНОСНО: Предложение за Регламент на Европейския парламент и на Съвета относно изискванията за хоризонтална киберсигурност за продукти с цифрови елементи и за изменение на Регламент (ЕС) 2019/1020, СОМ (2022) 454, 15 септември 2022 г. - т. 10 от Годишната работна програма на Народното събрание по въпросите на Европейския съюз (2022 г.) и Рамкова позиция на Република България по него, 48-202-00-13, внесена от Министерски съвет на 15 ноември 2022 г.

- I.** Предложение за Регламент на Европейския парламент и на Съвета относно изискванията за хоризонтална киберсигурност за продукти с цифрови елементи и за изменение на Регламент (ЕС) 2019/1020, СОМ/2022/0454, е проект на законодателен акт на Европейската комисия **от 15 септември 2022 г.** Актът е предаден на националните парламенти на държавите-членки на **24 октомври 2022 г.**

Съгласно Протокол № 2 от Договора за функционирането на Европейския съюз (ДФЕС) относно прилагането на принципите на субсидиарност и на пропорционалност, и правомощията на Народното събрание в рамките на заложения в чл. 6 от ДФЕС срок, **Комисията по въпросите на Европейския съюз (КВЕС)** на свое редовно заседание, проведено **на 15 декември 2022 г., обсъди** Предложение за Регламент на Европейския парламент и на Съвета относно изискванията за хоризонтална киберсигурност за продукти с цифрови елементи и за изменение на Регламент (ЕС) 2019/1020, СОМ/2022/454, **междунституционален номер 2022/0272 (COD)**, включено като т. 10 от Годишната работна програма на Народното събрание по въпросите на Европейския съюз за 2022 г.

В заседанието на КВЕС взеха участие г-н Атанас Мазнев - заместник-министър на електронното управление, г-н Константин Азов - началник на политическия кабинет на министъра, г-жа Гергана Колешанска - директор "Политики на е-управление", г-жа Рени Борисова - дирекция "Политики на е-управление", Боян Григоров - дирекция "Мрежова и информационна сигурност" в Министерство на електронното управление, както и народният представител и заместник-председател на Комисията по електронно управление и информационни технологии г-н Божидар Божанов.

- II. Предложението за Регламент** има две основни цели. Едната от тях е да се създадат условия за разработване на защитени продукти с цифрови елементи, като се гарантира, че на пазара се пускат хардуерни и софтуерни продукти с по-малко уязвимости, както и че производителите се отнасят сериозно към защитата през целия жизнен цикъл на продукта. Втората е създаването на условия, които позволяват на ползвателите да вземат предвид киберсигурността при избора и използването на продукти с цифрови елементи.

Предложението на Регламента предвижда и четири специфични цели. На първо място това е гарантирането, че производителите подобряват защитата на продуктите с цифрови елементи още от етапа на проектиране и разработване и през целия жизнен цикъл. Втората е осигуряването на съгласувана рамка за киберсигурност, която улеснява спазването на изискванията от производителите на хардуер и софтуер. Третата е повишаването на прозрачността на характеристиките за защитата на продуктите с цифрови елементи. Четвъртата е предоставянето на възможност на предприятията и потребителите да използват продуктите с цифрови елементи по безопасен начин.

Съгласно оценката на въздействие, извършената от Европейската комисия, съществуват четири варианта на политиката за постигане на общата цел на предложението. Предпочетен от Европейската комисия е вариант 4, който би гарантирал определянето на специфични хоризонтални изисквания за киберсигурност за всички продукти с цифрови елементи, които се пускат или предоставят на вътрешния пазар.

В обобщение предложението за регламент дава възможност държавите членки и съответно ЕС в цялост да преодолеят съществуващи недостатъци и фрагментация в областта на киберсигурността.

- III. Съгласно **Рамковата позиция, внесена от Министерски съвет**, Република България приветства предложението за Регламент на Европейския парламент и на Съвета относно изискванията за хоризонтална киберсигурност за продукти с цифрови елементи и за изменение на Регламент (ЕС) 2019/1020, COM/2022/454, като го счита за положително, навременно и необходимо. Изразява се подкрепа към целите, заложи в представеното от Европейската комисия предложение във всички посочени направления, и в крайна сметка внедряване на изисквания за киберсигурност за пускане на продукти с цифрови елементи на пазара на Съюза. Уеднаквяването на практиките и повишените мерки за киберсигурност в продуктите с цифрови елементи ще имат положително влияние за повишаване на хармонизацията и постигане на нужната сигурност в Съюза. **Същевременно Република България ще настоява за недопускане налагането на излишна административна тежест и ненужни ангажименти за икономическите оператори.** Страната изказва скептицизъм и по отношение на предвидените правомощия на ЕК да приема с делегиран акт изменения в приложението със списъка на критичните продукти с цифров елемент, като добавя нови категории или оттегля съществуващи такива от списъка. В тази връзка Република България ще поддържа позиция за неприемане с делегирани актове на съществени изменения в регламента и ще настоява за използване като правен инструмент на акт за изпълнение.

След приемането на настоящето предложение за Регламент на Европейския парламент и на Съвета относно изискванията за хоризонтална киберсигурност за продукти с цифрови елементи и за изменение на Регламент (ЕС) 2019/1020, COM/2022/454, може в изключително кратък срок да е необходимо да бъдат определени съществуващи органи и/или да създадат нови такива, изпълняващи задачите, уредени в законодателството, което ще наложи реално оценка на възможностите на национално ниво, както и промяна в националното законодателство и осигуряване на финансови средства за съответните дейности. Българската страна сочи, че заложените срокове следва да бъдат изпълними и да

съответстват на степента на готовност и на държавите членки да прилагат това ново законодателство.

За прилагането на регламента ще е необходимо създаването на органи, отговарящи за надзор на пазара и нотифициращ орган. От позицията става ясно, че към настоящия момент в страната не съществуват такива органи и ще е необходимо да се осигури административен капацитет и финансов ресурс за прилагане на задълженията на България по този регламент.

Въпреки, че предложеният регламент след окончателното си приемане ще се прилага пряко във всички държави членки, е необходимо да се направят изменения в Закона за киберсигурност, с които да се предвидят мерки по прилагането му.

- IV. Горепосоченото Предложение за Регламент е разгледано от Комисията по икономическа политика и иновации (КИПИ) на 30 ноември 2022 г. В своя доклад КИПИ посочва, че подкрепя рамковата позиция и счита, че предложението за Регламент съответства на принципите на субсидиарност и пропорционалност, но при финализиране на текста на предложението за регламент е необходимо да се вземат предвид избягване на свръхрегулацията, запазване на правото на избор и информираност на потребителите, запазване на конкуренцията между сертифицирани и несертифицирани продукти и непрекомерността на разходите за малкия бизнес.
- V. След състоялото се обсъждане по предложение за Регламент на Европейския парламент и на Съвета относно изискванията за хоризонтална киберсигурност за продукти с цифрови елементи и за изменение на Регламент (ЕС) 2019/1020, СОМ (2022) 454, вземайки предвид становищата на парламентарните комисии, Народното събрание на Република България, чрез Комисията по въпросите на Европейския съюз изразява следното **СТАНОВИЩЕ**, което да бъде изпратено до европейските институции, в рамките на политическия диалог:
1. КВЕС приветства усилията на Европейската комисия да гарантира киберсигурността на продуктите с цифрови елементи, както и последващото развитие на темата.
 2. КВЕС отчита, че предложението за изменения на Регламента ще допринесе за насърчаване на националните производители, доставчици и икономически оператори за изграждане на кибер устойчива национална екосистема, която да е хармонизирана в европейски контекст. Наред с това обаче за успешната имплементация на разпоредбите относно налагането на санкции ще са необходими значителен наличен капацитет и нормативни изменения.
 3. КВЕС счита, че е **спазен принципът на субсидиарност**, съгласно чл. 5, параграф 3 от Договора за Европейския съюз (ДЕС), но при финализиране на текста на предложението за регламент е необходимо да се вземат предвид избягване на свръхрегулацията, запазване на правото на избор и информираност на потребителите, запазване на конкуренцията между сертифицирани и несертифицирани продукти и непрекомерността на разходите за малкия бизнес.
 4. КВЕС изразява мнение, че **предложението за регламент съответства на принципа на пропорционалност**, определен от чл. 5, параграф 4 от ДЕС, тъй като с предложението не се въвеждат никакви мерки, надхвърлящи необходимото за постигането на основните цели на настоящата програма.

Бяха направени следните бележки по време на заседанието:

4.1. Относно чл. 10, параграф 4 от предложения регламент, задължението за предоставяне на гаранции от страна на производителя е непропорционално поради високата сложност на съвременните технологични продукти. Такива гаранции могат да бъдат единствено частични, в зависимост от спецификата на съответния продукт.

4.2. Относно чл. 10, параграф 6 от предложения регламент, за да бъдат постигнати целите на нормата, следва да бъде предвидено, че лицензионните модели не могат да оказват влияние върху предоставянето на обновления за отстраняване на уязвимости, тъй като съществува риск производители да обвържат заплащането на годишен абонамент с получаването на обновления, отстраняващи открити уязвимости.

4.3. Относно чл. 11, за постигане на поставените цели е необходимо информацията за установени уязвимости да се публикува в публично достъпни бази данни за уязвимости от ENISA или от производителите.

4.4. Относно чл. 15, непропорционално е изискването вносител да се счита за производител ако само продава съответния продукт под своя търговска марка (т.нар. whitelabeling). Това би ограничило сериозно модела на whitelabeling поради фактическата невъзможност на вносителя да влияе върху продукта и да се увери в неговите параметри, отнасящите се до сигурността до степен, в която да поеме цялата отговорност за това. Втората хипотеза, а именно в случаите, в които вносителят извършва сериозни модификации, е пропорционална и следва да бъде запазена.

5. С оглед на бързото развитие на технологиите и ускоряването на дигитализацията и дигиталната трансформация, както и силния трансграничен характер на киберсигурността и нарастващите трансгранични инциденти при всички сектори и продукти, **КВЕС приветства предложението за Регламент** на Европейския парламент и на Съвета относно изискванията за хоризонтална киберсигурност за продукти с цифрови елементи и за изменение на Регламент (ЕС) 2019/1020. То ще допринесе за повишаване на киберсигурността на продукти с цифрови елементи, което от своя страна ще повиши степента на доверие сред потребителите и привлекателността на продуктите на ЕС с цифрови елементи. Освен това предложението ще бъде от полза и за вътрешния пазар чрез предоставяне на правна сигурност и постигане на равни условия за икономическите оператори, отговорни за продукти с цифрови елементи.

С оглед на гореизложеното, след състоялото се обсъждане в КВЕС, докладът и становището към него бяха приети с 9 гласа „за“, 0 гласа „против“ и 0 гласа „въздържал се“.

**ПРЕДСЕДАТЕЛ НА
КОМИСИЯТА ПО ВЪПРОСИТЕ НА ЕС:**

ДЕНИЦА СИМЕОНОВА