Council of the European Union

Brussels, 21 December 2022
(OR. en, bg)

16249/22

Interinstitutional File:
2022/0272(COD)

CYBER 415
JAI 1725
DATAPROTECT 375
TELECOM 540
MI 973
CSC 604
CSCI 208
IA 233
CODEC 2073
INST 468
PARLNAT 196

COVER NOTE

From:	The Bulgarian National Assembly
date of receipt:	19 December 2022
To:	General Secretariat of the Council
Subject:	Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on horizontal cybersecurity requirements for products with digital elements and amending Regulation (EU) 2019/1020 [12429/22 - COM (2022) 454] - Opinion on the application of the Principles of Subsidiarity and Proportionality

Delegations will find attached the opinion of the Bulgarian National Assembly followed by a courtesy English translation.

РЕПУБЛИКА БЪЛГАРИЯ

ЧЕТИРИДЕСЕТ И ОСМО НАРОДНО СЪБРАНИЕ

КОМИСИЯ ПО ВЪПРОСИТЕ НА ЕВРОПЕЙСКИЯ СЪЮЗ

Д О К Л А Д

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, COM (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, COM/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, COM/2022/454**, междуинституционален 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, заложени 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, COM (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:

ДЕН Електронно подписан документ от : DENITSA DIMITROVA SIMEONOVA
Дата : 22/12/16 15:33:31+0200
В съответствие с eIDAS.

REPUBLIC OF BULGARIA

THE FORTY-EIGHT NATIONAL ASSEMBLY

COMMITTEE ON EUROPEAN UNION AFFAIRS

R E P O R T

ON: **Proposal for a Regulation of the European Parliament and of the Council on horizontal cybersecurity requirements for products with digital elements and amending Regulation (EU) 2019/1020, COM (2022) 454, 15 September 2022 - Item 10 of the Annual Work Programme of the National Assembly on European Union Affairs (2022) and the Framework Position of the Republic of Bulgaria thereon, 48-202-00-13, submitted by the Council of Ministers on 15 November 2022.**

I. Proposal for a Regulation of the European Parliament and of the Council on horizontal cybersecurity requirements for products with digital elements and amending Regulation (EU) 2019/1020, COM/2022/0454, is a draft legislative act of the European Commission **of 15 September 2022.** The act was submitted to the national parliaments of the Member States on **24 October 2022.**

Pursuant to Protocol No 2 of the Treaty on the Functioning of the European Union (TFEU) on the application of the principles of subsidiarity and proportionality and the powers of the National Assembly within the time limit laid down in Article 6 of TFEU, **the Committee on European Union Affairs** (CEUA), at its regular meeting held **on 15 December 2022, discussed** a Proposal for a Regulation of the European Parliament and of the Council on horizontal cybersecurity requirements for products with digital elements and amending Regulation (EU) 2019/1020, COM/2022/454**, interinstitutional number 2022/0272 (COD)**, included as item 10 of the Annual Work Programme of the National Assembly on European Union Affairs for 2022.

Mr. Atanas Maznev - Deputy Minister of e-Government, Mr. Konstantin Azov - Head of the Political Cabinet of the Minister, Ms. Gergana Kolesanska - Director "Policies of e-Government", Ms. Reni Borisova - Directorate "Policies of e-Government", Mr. Boyan Grigorov - Directorate "Network and Information Security" at the Ministry of e-Government, as well as the Member of the National Assembly and Vice-President of the Committee on e-Government and Information Technology Mr. Bozhidar Bozhanov took part in the meeting of the CEUA.

II. **The proposal for a Regulation** has two main objectives. One of them is to create conditions for the development of secure products with digital elements, ensuring that hardware and software products with fewer vulnerabilities are placed on the market, and that manufacturers take protection throughout the product life cycle seriously. The second one is the creation of conditions enabling users to take into account cybersecurity when selecting and using products with digital elements.

The proposal for a Regulation also provides for four specific objectives. First and foremost, this is to ensure that manufacturers improve the protection of products with digital elements right from the design and development stage and throughout the life cycle. The second one is to provide a coherent cybersecurity framework that facilitates

compliance by hardware and software manufacturers. The third one is to increase the transparency of product protection features with digital elements. The fourth one is to enable businesses and consumers to use products with digital elements in a safe way.

According to the impact assessment carried out by the European Commission, there are four policy options to achieve the overall objective of the proposal. A preferred option by the European Commission is option 4, which would ensure that specific horizontal cybersecurity requirements are set for all products with digital elements that are placed or made available on the internal market.

In summary, the proposal for a Regulation enables Member States and thus the EU as a whole to address existing shortcomings and fragmentation in the field of cybersecurity.

III. Pursuant to the **Framework Position submitted by the Council of Ministers**, the Republic of Bulgaria welcomes the proposal for a Regulation of the European Parliament and of the Council on horizontal cybersecurity requirements for products with digital elements and amending Regulation (EU) 2019/1020, COM/2022/454 by considering it positive, timely and necessary. Support is expressed for the objectives set out in the proposal presented by the European Commission in all directions and ultimately the introduction of cybersecurity requirements for placing products with digital elements on the Union market. The alignment of practices and increased cybersecurity measures in products with digital elements will have a positive impact on increasing harmonisation and achieving the necessary security in the Union. **At the same time, the Republic of Bulgaria will insist on preventing the imposition of unnecessary administrative burdens and unnecessary commitments for economic operators.** The country also expresses scepticism about the envisaged powers of the EC to adopt by a delegated act amendments in the annexe with the list of critical products with digital elements, adding new categories or withdrawing existing ones from the list. In this regard, the Republic of Bulgaria will maintain a position for non-adoption by delegated acts of substantial amendments to the Regulation and will insist on the use of an implementing act as a legal instrument.

Following the adoption of this proposal for a Regulation of the European Parliament and of the Council on horizontal cybersecurity requirements for products with digital elements and amending Regulation (EU) 2019/1020, COM/2022/454, it may be necessary to rapidly designate existing bodies and/or create new ones to carry out the tasks set out in the legislation, which will effectively require an assessment of the possibilities at a national level, as well as a change in the national legislation and the provision of financial resources for the activities concerned. Bulgaria indicates that the deadlines set should be feasible and consistent with the level of readiness of the Member States to implement this new legislation.

The implementation of the Regulation will require the establishment of market surveillance authorities and a notifying body. It is clear from the position that at the moment there are no such bodies in the country and it will be necessary to provide administrative capacity and financial resources for the implementation of Bulgaria's obligations under this Regulation.

Although the proposed Regulation will apply directly in all Member States after its final adoption, it is necessary to amend the Cybersecurity Act to provide for implementing measures.

IV. The above proposal for a Regulation was examined by the Committee on Economic Policy and Innovation (CEPI) on 30 November 2022. In its report, CEPI states that it supports the framework position and considers that the proposal for a Regulation is in line with the principles of subsidiarity and proportionality, but when finalising the text of the proposal for a Regulation, it is necessary to take into account the avoidance of over-regulation, the preservation of consumer choice and information, the preservation of competition between certified and uncertified products and the undue cost of small business.

V. Following a discussion on a proposal for a Regulation of the European Parliament and of the Council on horizontal cybersecurity requirements for products with digital elements and amending Regulation (EU) 2019/1020, COM (2022) 454, taking into account the opinions of the parliamentary committees, the National Assembly of the Republic of Bulgaria, through the Committee on European Union Affairs, expresses the following OPINION to be sent to the European institutions in the framework of the political dialogue:

1. The CEUA welcomes the efforts of the European Commission to ensure cybersecurity of products with digital elements, as well as the subsequent development of the topic.
2. The CEUA recognises that the proposal for amendments to the Regulation will contribute to encouraging national producers, suppliers and economic operators to build a cyber resilient national ecosystem that is harmonised in a European context. In addition, however, the successful implementation of the sanctioning provisions will require significant available capacity and regulatory changes.
3. The CEUA considers that **the principle of subsidiarity has been observed** pursuant to Article 5(3) of the Treaty on European Union (TEU), but when finalizing the text of the proposal for a Regulation, it is necessary to take into account the avoidance of over-regulation, preservation of the right of choice and information of consumers, preservation of competition between certified and non-certified products and the non-excessiveness of costs for small businesses.
4. The CEUA expresses the opinion that the **proposal for a Regulation is in line with the principle of proportionality**, as set out in Article 5(4) of TEU, as the proposal does not introduce any measures that go beyond what is necessary to achieve the main objectives of this programme.

The following comments were made at the meeting:

4.1. With regard to Article 10(4) of the proposed Regulation, the obligation to provide guarantees by the manufacturer is disproportionate due to the high complexity of modern technological products. Such guarantees may only be partial, depending on the specifics of the product concerned.

4.2. With regard to Article 10(6) of the proposed Regulation, in order to achieve the objectives of the Regulation, it should be provided that licensing models cannot have an impact on the provision of updates to remedy vulnerabilities, as there is a risk that manufacturers will make the payment of an annual subscription conditional on receiving updates that remedy open vulnerabilities.

4.3. With regard to Article 11, in order to achieve the set objectives, it is necessary to publish the information on identified vulnerabilities in publicly available vulnerability databases by ENISA or by the producers.

4.4. With regard to Article 15, it is disproportionate to consider an importer as a manufacturer only if it sells the product under its trademark (the so-called whitelabeling). This would severely limit the whitelabeling model due to the factual impossibility of the importer to influence the product and to ascertain its security parameters to the extent that it assumes full responsibility for it. The second hypothesis, namely where the importer makes serious modifications, is proportionate and shall be maintained.

5. In view of the rapid development of technologies and the acceleration of digitalisation and digital transformation, as well as the strong cross-border nature of cybersecurity and increasing cross-border incidents in all sectors and products, **the CEUA welcomes the proposal for a Regulation** of the European Parliament and of the Council on horizontal cybersecurity requirements for products with digital elements and amending Regulation (EU) 2019/1020. It will contribute to enhancing cybersecurity of products with digital elements, which in its turn will increase consumer confidence and the attractiveness of EU products with digital elements. Furthermore, the proposal will also benefit the internal market by providing legal certainty and a level playing field for the economic operators responsible for products with digital elements.

In view of the above, following a discussion conducted at the CEUA, the report and <u>its opinion</u> were adopted by 9 votes "in favour", 0 votes "against" and 0 "abstentions".

CHAIRPERSON OF
THE COMMITTEE ON EU AFFAIRS:
DENITSA SIMEONOVA

Електронно подписан документ от : DENITSA DIMITROVA SIMEONOVA
Дата : 22/12/19 12:53:51+0200
В съответствие с eIDAS.