Проект!

Мотиви към проекта на Закон за изменение и допълнение на Наказателно-процесуалния кодекс

1. Причини, които налагат приемането на предложения проект на Закон за изменение и допълнение на Наказателно-процесуалния кодекс

С настоящия проект на Закон за изменение и допълнение на Наказателно-процесуалния кодекс (ЗИД на НПК) се предлага приемането на необходимите изменения и допълнения в националното законодателство с оглед:

- привеждането му в съответствие с разпоредбите на Втория допълнителен протокол към Конвенцията за престъпленията в кибернетичното пространство на Съвета на Европа и за целите на последващата ратификация на Протокола;
- осигуряване на прилагането на Регламент (ЕС) 2023/1543 на Европейския парламент и на Съвета от 12 юли 2023 година относно европейските заповеди за предоставяне и европейските заповеди за запазване на електронни доказателства в рамките на наказателните производства и за изпълнението на наказания лишаване от свобода вследствие на наказателни производства;
- въвеждането на изискванията на Директива (ЕС) 2023/1544 на Европейския парламент и на Съвета от 12 юли 2023 година за установяване на хармонизирани правила относно определянето на определени форми на установяване и определянето на представители за целите на събирането на електронни доказателства по наказателни производства.
- изпратено от Европейската комисия на 27 март 2026 г. официално уведомително писмо за образуване на процедура за нарушение № 2026/0155 по чл. 258 от Договора за функционирането на Европейския съюз. Процедурата е за неуведомяване в срок на Европейската комисия за мерките за пълно транспониране в българското законодателство на Директива (ЕС) 2023/1544 на Европейския парламент и на Съвета от 12 юли 2023 година за установяване на хармонизирани правила относно определянето на определени форми на установяване и определянето на представители за целите на събирането на електронни доказателства по наказателни производства. Срокът за транспониране на директивата е бил 18 февруари 2026 г.

2. Цели на предложения проект на акт за изменение и допълнение на Наказателно-процесуалния кодекс

Целта на предложения проект на Закон за изменение и допълнение на Наказателно-процесуалния кодекс е привеждане на вътрешното законодателство в съответствие с европейски и международни актове в областта на наказателнопроцесуалното право, практиката на Съда на Европейския съюз и Европейския съд по правата на човека, както

и повишаване на ефективността на правната уредба и осъвременяването ѝ с оглед развитието на информационните технологии и способите за комуникация.

3. Същност на законодателните промени

Предложенията могат да бъдат разделени в няколко категории:

3.1. Привеждане на националното законодателство в съответствие с разпоредбите на Втория допълнителен протокол към Конвенцията в кибернетичното пространство на Съвета на Европа

Конвенцията за престъпленията в кибернетичното пространство от 2001 г. („Конвенцията“) е основополагаща глобална правна рамка за сътрудничество и противодействие на престъпленията в киберпространството. Тя е ратифицирана от 80 държави - 45 държави - членки на Съвета на Европа (СЕ), в това число България, и 35 държави извън Съвета на Европа. Поради всеобщо признатата необходимост от приемането на мерки, които да ускорят трансграничния обмен на електронни доказателства за целите на наказателното производство, в рамките на Съвета на Европа през м. юни 2017 г. беше инициирано разработването на Втори допълнителен протокол към Конвенцията за засилено сътрудничество и разкриване на електронни доказателства.

Протоколът следва да послужи като инструмент за засилване на сътрудничеството между публичния и частния сектор за борба срещу престъпността с оглед на значителните предизвикателства пред съдебните и разследващите органи - нови форми на изпълнителни деяния на традиционни престъпни прояви, все по-съществени вредни последици от наднационален характер, условия за по-лесно укриване на недобросъвестните лица и др. Протоколът беше официално открит за подписване на международна конференция на 12-13 май 2022 г. в гр. Страсбург, Франция и подписан от редица държави, включително и България.

С оглед на необходимостта от засилено и успешно сътрудничество между държавните органи и субектите в частния сектор, чрез разпоредбите на Втория допълнителен протокол се цели създаването на по-голяма правна сигурност по отношение на условията, при които доставчиците на услуги могат да отговарят на непосредствени искания, отправени от съдебните органи за целите на предоставяне на достъп до конкретни данни в цифров формат. Вторият допълнителен протокол създава възможност за директна комуникация между компетентните органи на една държава с доставчик на услуги, който се намира на територията на друга държава.

Протоколът включва и разпоредби от традиционен тип за оказване на сътрудничество между съдебните органи на съдоговарящите страни, като последните разполагат с правото да изискват предоставянето или запазването на данни от доставчици, които попадат в тяхната юрисдикция. По този ред ще се прилагат две процедури – за изпълнение на заповед за бързо предоставяне на данни за абоната и на данни за трафика, както и специална процедура за бързо разкриване на съхранени компютърни данни в спешни случаи.

- **Оправомощаване на националните компетентни органи (съд, прокуратура, Министерството на вътрешните работи) в съответствие с разпоредбите на Протокола**

Правомощия на органите в наказателното производство

В съответствие с чл. 6 и 7 от Протокола с предложения чл. 159б в НПК се въвеждат правомощия за органите на досъдебното производство и за съда да изискват директно от доставчик на услуги на информационното общество и от предприятие, предоставящо обществени електронни съобщителни мрежи и/или услуги, които се намират на територията на друга държава, която е страна по Протокола, данни за регистрация на домейн и/или данни за абоната на компютърно-информационна услуга („данни за абоната“).

Същевременно Протоколът предвижда и алтернативен режим, който се доближава до традиционните методи на международното сътрудничество в наказателноправната област относно предоставянето на данни за абоната и данни за трафика. За целите на привеждането на вътрешното право в съответствие с член 8 от Протокола, който урежда този въпрос, се създава чл. 159в НПК, чрез който съдът в съдебното производство или наблюдаващият прокурор в досъдебното производство се оправомощават да изискват от компетентния орган на другата държава горепосочените два вида данни. По отношение на трафичните данни искането се изпраща след мотивирано съдебно разпореждане в съответствие с приложимата по националното законодателство процедура по чл. 159а, ал. 2 – 5 НПК.

В реципрочните случаи съгласно Протокола, когато искането е изпратено от друга държава към България, окръжната прокуратура по седалището на доставчика или предприятието (в съответствие с направеното съобщение по член 8, параграф 10, буква „б“ от Протокола) предоставя на компетентния орган на другата държава данни за абоната и/или данни за трафика. За данните на трафика отново се прилагат чл. 159а, ал. 2 - 5 НПК, като разрешението се предоставя от председателя на окръжния съд по седалището на предприятието или на доставчика или от оправомощен от него съдия с мотивирано разпореждане. Когато искането се отнася до дейността на предприятия и доставчици, чиито седалища се намират в районите на повече от един окръжен съд, мотивираното разпореждане се издава от председателя на Софийския градски съд или от оправомощен от него съдия по искане на Софийската градска прокуратура.

Правомощия на органите извън наказателното производство

Тъй като разпоредбите на Протокола не се ограничават единствено до действията на компетентните органи в рамките на наказателното производство, в заключителните разпоредби на законопроекта се предлагат допълнения в Закона за Министерството на вътрешните работи. С предложенията изрично се уреждат правомощията на Главна дирекция „Борба с организираната престъпност“ като звено за контакт 24/7 по член 35 от Конвенцията за престъпления в кибернетичното пространство и орган по член 8, параграф 10, букви „а” и „б“ от Протокола, който съдейства на оперативно-

издирвателните органи на Министерството на вътрешните работи (МВР) при осъществяване на дейностите, произтичащи от текстовете на Протокола.

В съответствие с членове 6 и 7 от Протокола органите на МВР се оправомощават да поискат от доставчик или предприятие, което се намира на територията на друга държава, да предоставят данни за регистрация на домейн и данни за абоната за целите на предотвратяването, разкриването и разследването на престъпления и издирването на лица. Поради по-високата чувствителност на данните за трафика те не се изискват директно от доставчика, а единствено чрез компетентния орган на другата държава и след писмено разрешение от председателя на съответния районен съд или от оправомощен от него съдия. Този режим се прилага и за данни за абоната, ако другата държава изисква искането за тях да бъде издадено под надзора на съдебен орган.

Всички искания от органите на МВР ще се изпращат чрез звеното за контакт 24/7 в Главна дирекция „Борба с организираната престъпност“ – централизирането на тази дейност е целесъобразно от гледна точка на естеството на международното сътрудничество, тъй като в противен случай ще бъде налице твърде широк кръг от изпращащи органи (ако бъдат изброени всички структури на МВР, посочени в Закона за електронните съобщения (ЗЕС). В подобен случай съществува по-голям риск компетентният орган на получаващата държава да се усъмни в автентичността на отправеното искане.

В ЗМВР се предвижда и в спешни случаи в съответствие с Протокола звеното за контакт 24/7 да може да поиска от доставчик на услуги на информационното общество или от предприятие, предоставящо обществени електронни съобщителни мрежи и/или услуги, данни, за чието предоставяне не е установен специален ред. Включването на този текст се налага поради следните съображения – понастоящем съгласно Конвенцията от 2001 г. след получаване на искане от звено за контакт 24/7 на друга държава Главна дирекция „Борба с организираната престъпност“ има право единствено да изиска запазването на данни, които впоследствие се предоставят на другата държава въз основа на молба за правна помощ (или Европейска заповед за разследване, ако молещата държава е членка на Европейския съюз). Член 9 от Втория допълнителен протокол предоставя възможност за съдействие без молба за правна помощ в спешни случаи, поради което звеното за контакт следва да бъде оправомощено да изисква директно получаване на данните, а не само тяхното запазване. Поради това е необходимо да се създаде допълнително правно основание извън случаите, в които има специален ред за предоставяне на данните (например реда за изискване на данни за трафика по ЗЕС).

- **Оправомощаване на субекти в частния сектор в съответствие с разпоредбите на Протокола**

В съответствие с член 6, параграф 2 и член 7, параграф 2 от Протокола се предлагат допълнения в Закона за електронната търговия (ЗЕТ) (създава се чл. 4в), както и в Закона за електронните съобщения (създаване на ал. 4 и 5 на чл. 251з), съгласно които доставчиците на услуги на информационното общество и предприятията, предоставящи обществени електронни съобщителни мрежи и/или услуги, предоставят директно на компетентен орган на друга държава данни за регистрация на домейн и данни за абоната

по негово искане, когато това е предвидено в Протокола. Същевременно се създава специална гаранция, според която всеки доставчик или предприятие ще има възможността да се консултира с Върховната касационна прокуратура при възникване на съмнение относно законосъобразността и автентичността на полученото искане.

Освен това за целите на последователното прилагане на всички разпоредби, произтичащи от привеждането на националното законодателство в съответствие с Протокола, в Закона за електронната търговия се създават и дефиниции на понятията „данни за регистрация на домейн“ и „данни за абоната“.

3.2. Осигуряване на прилагането на Регламент (ЕС) 2023/1543 и въвеждане на изискванията на Директива (ЕС) 2023/1544

- **Наказателно-процесуален кодекс**

В член 3, точка 10 от Регламент (ЕС) 2023/1543 се въвежда категория „*данни, поискани единствено с цел идентифициране на ползвателя*“. Според дефиницията това са „*IP адреси и, когато е необходимо, съответните портове при източника и времеви печат, а именно датата и часа или технически еквиваленти на тези идентификатори и свързаната с тях информация, когато това се изисква от правоохранителните или от съдебните органи единствено с цел идентифициране на ползвателя в конкретно наказателно разследване*.“ За тях Регламентът създава по-облекчен режим за събиране в рамките на наказателното производство, който е приравнен на правилата за потребителските данни. За целите на осигуряването на прилагането на Регламента и тъй като сходна категория не съществува в националното ни право, се създава ал. 7 на чл. 159а НПК, съгласно която ал. 1 - 6 на същия член не се прилагат, когато данните по ал. 1, т. 1, 3 и 5 се изискват само с цел установяването на самоличността на потребителя и не са свързани с осъществяването на повиквания или предаването на съобщения, като целта трябва задължително да се посочи в искането. Останалите данни (по чл. 159а, ал. 1, т. 2, 4 и 6 НПК) по-скоро винаги имат отношение към осъществяването на повиквания, предаването на съобщения или други действия, например свързани с функционирането на мобилните апарати в рамките на съобщителната мрежа. Когато изискванията на новосъздадената ал. 7 са изпълнени, данните ще се събират не на основание чл. 159а, а в съответствие с чл. 159 НПК.

- **Закон за електронните съобщения и Закон за електронната търговия**

За целите на въвеждането на изискванията на Директива (ЕС) 2023/1544 в Закона за електронните съобщения (по отношение на предприятията, предоставящи обществени електронни съобщителни мрежи и/или услуги) и в Закона за електронната търговия (спрямо доставчиците на услуги на информационното общество) се създават нови разпоредби относно определянето на адресат за целите на събирането на електронни доказателства по наказателни производства (в законопроекта изрично е уредена хипотеза и за заварените случаи). Тези две категории попадат в приложното поле на двата акта - съответно член 2, точка 1 от Директива (ЕС) 2023/1544 и член 3, точка 3 от Регламент

(ЕС) 2023/1543 с изключение на предприятията и доставчиците, които предоставят услуги единствено на територията на Република България. Допълват се и административнонаказателните разпоредби на двата закона във връзка със случаите, в които предприятията и доставчиците нарушават задълженията, които произтичат от разпоредбите, които транспонират Директива (ЕС) 2023/1544, както и тези, които произтичат от непосредственото приложение на Регламент (ЕС) 2023/1543.

За целите на осигуряване на прилагането на чл. 19 от Регламент (ЕС) 2023/1543 се предвижда в шестмесечен срок от влизането в сила на закона Комисията за регулиране на съобщенията да изгради и поддържа инфраструктура (точка за достъп до системата e-CODEX), която дава възможност за цифрова свързаност в рамките на Европейския съюз и чрез която адресатите, определени по реда на Закона за електронните съобщения и Закона за електронната търговия, ще се свържат с децентрализираната информационна система, за да получават удостоверенията за европейска заповед за предоставяне и запазване на електронни доказателства.

Въпреки че съгласно Закона за електронните съобщения и Закона за електронната търговия по отношение на доставчиците на услуги, които попадат в приложното поле на Регламент (ЕС) 2023/1543 и Директива (ЕС) 2023/1544, контролна дейност освен Комисията за регулиране на съобщенията осъществява и Комисията за защита на потребителите, създаването на две отделни точки за достъп би било нецелесъобразно от гледна точка на необходимите финансови средства.

В допълнение е необходимо да се уточни защо не е възможно да се ползват вече изградените e-Codex точки към прокуратурата, Висшия съдебен съвет и Министерството на правосъдието. Съществуващите e-Codex точки са част от информационната инфраструктура на посочените органи и са предназначени да обслужват обмена на информация, свързана с дейността на съответните институции. Наличната инфраструктура е изградена за конкретни функционални и организационни нужди, като параметрите ѝ са съобразени както с очакваното натоварване, така и с приложимите изисквания за информационна и киберсигурност. Допускането на външни доставчици на услуги до същата инфраструктура би създало предпоставки за нарушаване на установените механизми за разделяне на мрежите, системите и обработваните данни.

Следва да се отчете и обстоятелството, че доставчиците на услуги представляват самостоятелни частноправни субекти с различно равнище на организационни и технически мерки за сигурност. При евентуално компрометиране на профил на доставчик би възникнала възможност за неоторизиран достъп до e-Codex точката, което от своя страна би могло да доведе до: нерегламентиран достъп до вътрешни информационни ресурси; разкриване или неправомерно обработване на чувствителна информация; засягане на автентичността, целостта и надеждността на обменяните данни и др.

Предоставянето на достъп на външни частни субекти би наложило радикална промяна в цялата политика за управление на достъпа, което е технически сложно, рисково и само по себе си би създало рискове за уязвимост. Съвременните стандарти за киберсигурност, вкл. препоръчваните от Агенцията на ЕС за киберсигурност (ENISA) и Европейската комисия, изискват отделни, изолирани точки на достъп за различни категории участници. Използването на една и съща точка за съдебни органи и частни

доставчици противоречи на принципа на разделяне на системата, мрежата или данните на независими една от друга зони, така че пробив в една част да не компрометира цялата система. Използването на обща точка би могло да бъде квалифицирано като неспазване на нормативните задължения, вкл. по Общия регламент за защита на данните (GDPR), както и като създаване на недопустим риск по отношение на киберсигурността.

Поради тези причини необходимостта от изграждането на нова e-Codex точка е не само технически обоснована, но и задължителна от гледна точка на сигурността. Това решение гарантира както ефективното прилагане на европейското законодателство, така и защитата на критичната инфраструктура.

- **Закон за Европейската заповед за разследване**

За целите на транспонирането на член 3, параграф 3 от Директива (ЕС) 2023/1544 в Закона за Европейската заповед за разследване се създава чл. 33а, съгласно който компетентният орган по изпълнението на Европейската заповед за разследване изпраща искането за предоставяне на съответните данни до адресата, определен от предприятието, предоставящо обществени електронни съобщителни мрежи или обществени електронни съобщителни услуги, или от доставчика на услуги на информационното общество по реда на предложените нови разпоредби в Закона за електронните съобщения и в Закона за електронната търговия.

- **Закон за защита на личните данни**

В административнонаказателните разпоредби на Закона за защита на личните данни се предвижда налагането на санкция, в случай че предприятие, предоставящо обществени електронни съобщителни мрежи или обществени електронни съобщителни услуги, доставчик на услуги на информационното общество или определен от тях адресат не изпълни задължение, произтичащо от член 13, параграф 4 от Регламент (ЕС) 2023/1543 (осигуряване на поверителността, опазването на тайната и цялостността на удостоверението за европейска заповед за предоставяне или на удостоверението за европейска заповед за запазване и на данните, които са предоставени или запазени), тъй като в тези случаи компетентен орган е Комисията за защита на личните данни.

3.3. Предложения, произтичащи от практиката на Съда на Европейския съюз и на Европейския съд по правата на човека

- **Уведомяване на засегнатото лице и правни средства за защита**

Съгласно Решение на Съда на Европейския съюз от 17 ноември 2022 г. (дело C-350/21) с предмет преюдициално запитване, отправено от Специализирания наказателен съд на основание член 15, параграф 1 от Директива 2002/58/ЕС[1] във връзка с чл. 7, 8 и 11

[1] Директива 2002/58/ЕС относно обработването на лични данни и защита на правото на неприкосновеност на личния живот в сектора на електронните съобщения.

и чл. 52, пар. 1 от Хартата на основните права на Европейския съюз, както и във връзка с чл. 13 и 54 от Директива (ЕС) 2016/680[2], същите трябва да се тълкуват в смисъл, че не допускат национална правна уредба, която предвижда достъп от страна на националните органи, компетентни в областта на разследването на престъпления, до законно запазени данни за трафик и данни за местонахождение, без да гарантира, че лицата, до чиито данни са имали достъп тези национални органи, са били уведомени за това в степента, предвидена от правото на Съюза, и без посочените лица да разполагат с правно средство за защита срещу неправомерен достъп до тези данни.

Проблемът относно липсата на специално правно средство за защита в рамките на уредбата за достъпа до данни за трафика е изтъкнат и в решението на Европейския съд по правата на човека от 11 януари 2022 г. по делото „Екимджиев и други срещу България“. В него се посочва, че не е налице средство за обезщетяване на лицата в случай на неправомерен достъп до данни.

Настоящият законопроект има за цел да разреши именно проблемите с липсата на уведомяване на засегнатото лице, както и с липсата на средство за защита на пострадалия от неправомерен достъп. Поради тази причина се предлагат допълнения в НПК (създава се чл. 159д „Уведомяване на засегнатото лице“) и в Закона за отговорността на държавата и общините за вреди (ЗОДОВ). Предложеният режим в ЗОДОВ следва логиката на отговорността на държавата за вреди от незаконосъобразно използване на специални разузнавателни средства по чл. 2, ал. 1, т. 7 и цели привеждане на законодателството в съответствие с минималните правозащитни стандарти в тази област. Предложеното допълнение е необходимо, защото не всички случаи на противозаконно събиране на трафични данни попадат в приложното поле на новия раздел IX от глава четиринадесета на НПК (във връзка с чл. 2, ал. 1, т. 10 ЗОДОВ) - например когато достъпът до данните се получава по реда на Закона за електронните съобщения.

3.4. Други предложения, свързани с повишаване на ефективността на правната уредба и осъвременяването ѝ с оглед развитието на информационните технологии и способите за комуникация

В законопроекта се предлага заличаването на думата „умишлени“ в ал. 2 на чл. 159а НПК (по отношение на видовете престъпления, за разследването на които могат да се събират данни за трафика). Изискването „тежки умишлени“ отива отвъд предписанията на чл. 34, ал. 2 от Конституцията, съгласно който изключение от принципа за неприкосновеност на тайната на кореспонденцията и на другите съобщения се допуска само с разрешение на съдебната власт, когато това се налага за разкриване или предотвратяване на тежки престъпления, без да посочва изрично формата на вина. По този начин компетентните органи се лишават от възможността да получават достъп до трафични данни, вкл. данни за местоположението, с оглед разкриването на извършени по непредпазливост тежки престъпления. Същевременно, в Наказателния кодекс

[2] Директива (ЕС) 2016/680 относно защитата на физическите лица във връзка с обработването на лични данни от компетентните органи за целите на предотвратяването, разследването, разкриването или наказателното преследване на престъпления или изпълнението на наказания и относно свободното движение на такива данни.

съществуват редица престъпни състави, при които настъпилият резултат от извършеното по непредпазливост деяние е достатъчно значителен (например пътнотранспортно произшествие с множество пострадали). Освен това с предложеното изменение се цели и уеднаквяване на правната уредба за събирането на данни с трафика с тази по Закона за електронните съобщения (чл. 251б, ал. 2).

В допълнение се предлагат и изменения в чл. 165 НПК с цел привеждането му в съответствие с новите реалности в областта на комуникацията, извършвана чрез информационните технологии. Тъй като огромната част от кореспонденцията в днешни дни е електронна, а в тези случаи хипотезата „недоставена“ е изключителна рядкост, запазването на думата „недоставена“ практически обезсмисля съществуването на ал. 3. Освен това понастоящем ал. 3 не се прилага за електронната поща, т.е. кореспонденция от електронна поща се събира само с предварително съдебно решение. Понятието в ал. 6 „електронна поща“ не отговаря на терминологията, която се използва в Закона за електронните съобщения, поради което се предлага приложното поле на чл. 165 НПК да се разшири чрез включване на всякаква кореспонденция чрез електронни съобщения, вкл. съдържанието на електронната поща, чрез допълнение на ал. 1.

С оглед на разширяването на приложното поле на ал. 3 и към електронната кореспонденция се създава възможност режимът за неотложност да се прилага спрямо всички тежки престъпления. По този начин във връзка с разследването на тежката престъпност ще се реши и проблемът, повдигнат например в Решение № 530 от 4.01.2012 г. на Върховния касационен съд - в съвременния свят при претърсване и изземване на компютърна информационна система (чл. 163, ал. 6 НПК) в условията на неотложност е твърде вероятно да се открият данни, които имат двойствена природа. От една страна те представляват компютърни данни по смисъла на НК, но от друга - могат да се приравнят на кореспонденция, за която е приложим редът по чл. 165 НПК, съгласно който в съответствие с действащата досега нормативна уредба тя може да се изземе единствено с предварително съдебно разпореждане (с изключение на терористичните престъпления и престъпните деяния по чл. 354а от Наказателния кодекс).

4. Очаквани резултати от прилагането на проекта на Закона за изменение и допълнение на Наказателно-процесуалния кодекс

Очакваните резултати от приемането на проекта на Закон за изменение и допълнение на Наказателно-процесуалния кодекс са:

- подобряване на трансграничния достъп до електронни доказателства чрез въвеждането на специален режим, съгласно който разследващите органи на държавите членки могат да се обръщат директно към доставчиците на услуги на територията на Европейския съюз във връзка с предоставянето и запазването на данни, необходими за целите на наказателния процес (чрез осигуряване на прилагането на Регламент (ЕС) 2023/1543);
- хармонизиране на вътрешното законодателство в съответствие с Директива (ЕС) 2023/1544, която установява правила за определянето на представител на доставчиците, които предлагат услуги на територията на Европейския съюз, който да

получава и изпълнява заповедите за предоставяне и запазване на данни по Регламент (ЕС) 2023/1543 (закриване на процедура за нарушение № 2026/0155);

- повишаване на ефективността на правната уредба и осъвременяването ѝ с оглед развитието на информационните технологии и способите за комуникация чрез привеждането ѝ в съответствие с разпоредбите на Втория допълнителен протокол към Конвенцията за престъпленията в кибернетичното пространство на Съвета на Европа и с практиката на Съда на Европейския съюз и Европейския съд по правата на човека.

Проектът на Закон за изменение и допълнение на Наказателно-процесуалния кодекс е включен в т. 66, мярка № 194 от Законодателната програма на Министерския съвет за периода май - юни 2026 г., приета с Решение на Министерския съвет № 414 от 20 май 2026 г.

5. Финансови и други средства, необходими за прилагането на новата уредба

Предложеният проект на акт ще окаже въздействие върху държавния бюджет и се придружава от финансова обосновка съгласно приложение № 2.1 на чл. 35, ал. 1, т. 4, буква „а“ от Устройствения правилник на Министерския съвет и на неговата администрация.

Общо необходимите допълнителни финансови средства за прилагане на проекта на акт са в размер 72 000 евро на годишна база, считано от 2027 г. Средствата са за изграждане и поддържане от страна на КРС на инфраструктура (точка за достъп до системата E-Codex) за целите на прилагането на Регламент (ЕС) 2023/1543, както и за разходи за персонал на експертите, които ще изпълняват възложените с проекта на ЗИД на НПК нови правомощия за КРС. Разпределени са както следва:

- за изграждане и поддръжка на точка за достъп до системата E-Codex – 31 000 евро за 2027 г. и всяка следваща година;

- за разходи за персонал – 41 000 евро за 2027 г. и всяка следваща година.

Разходите не са предвидени по бюджета на Комисията за регулиране на съобщенията и в тази връзка е необходимо осигуряването им с цел обезпечаване на новите дейности, произтичащи от промените с предложения проект на ЗИД на НПК.

Законопроектът не съдържа разпоредби, свързани с въвеждането на регулаторни режими.

Проектът на закон съдържа разпоредби, въвеждащи актове на Европейския съюз, поради което е изготвена таблица за съответствие с правото на ЕС.

Към законопроекта е приложена справка за съответствието му с Европейската конвенция за защита на правата на човека и основните свободи и с практиката на Европейския съд по правата на човека.