

Формуляр за частична предварителна оценка на въздействието*
(Приложете към формуляра допълнителна информация/документи)

Институция: Министерство на здравеопазването	Нормативен акт: Проект на Постановление на Министерския съвет за изменение и допълнение на Устройствения правилник на Министерството на здравеопазването
За включване в законодателната/оперативната програма на Министерския съвет за периода: Проектът не е включен в оперативната програма на Министерския съвет.	Дата: м. ноември 2019 г.
Контакт за въпроси: Невена Цветкова, главен юрисконсулт в дирекция „Правна“	Телефон: 02 9301151

Дефиниране на проблема:

1.1. Кратко опишете проблема и причините за неговото възникване. Посочете аргументите, които обосновават нормативната промяна.

Поради недостатъчното равнище на защита срещу инциденти, рискове и заплахи в областта на мрежовата и информационната сигурност в Европейския съюз, в т.ч. и България, възпрепятстващо правилното функциониране на вътрешния пазар, е приет Законът за киберсигурност.

Законът установява цялостна система за координация и взаимодействие между компетентните органи в областта на киберсигурността, както и правила за докладване на инциденти в киберсигурността, засягащи административните органи, операторите на съществени услуги и доставчиците на цифрови услуги в отношенията на национално равнище, както и между държавите членки на Европейския съюз.

Законът даде нова рамка, като утвърди общите понятия в киберсигурността, определи ключовите за държавата сектори, компетентните органи в областта на киберсигурността, техните функции и правомощия, както и дейностите по предприемане на необходимите мерки за постигане на високо общо ниво на сигурност на мрежите и информационните системи във всички сегменти на киберпространството и на всички нива, така че да се подобри функционирането на вътрешния пазар. Създаде се един общ инструментариум за своевременно, бързо и адекватно споделяне на информация за инциденти и минимизиране на негативните последици.

С Решение № 192 на Министерския съвет от 2019 г. са определени административните органи, към които се създават национални компетентни органи по мрежовата и информационната сигурност в изпълнение на изискването на чл. 16, ал. 1 от Закона за киберсигурност. Определянето на тези административни органи е етап от сформирването на органите, на които законът възлага изпълнението на мерките и задачите, свързани с опазването и подобряването на мрежовата и информационната сигурност с цел ограничаване на мащаба, честотата и въздействието на киберинциденти и подобряване на надеждността, устойчивостта и ефективността на мрежите и информационните системи на всички субекти в обхвата на закона.

С цитираното решение министърът на здравеопазването е определен за административен орган, към който се създава национален компетентен орган по мрежова и информационна сигурност за сектор „Здравеопазване“.

Съгласно § 5, ал. 1, т. 1 от преходните и заключителни разпоредби на Закона за киберсигурност, административните органи по чл. 16, ал. 1 от закона в срок до два месеца от приемането на решението на Министерския съвет създават национални компетентни органи и секторни екипи към тях по чл. 18, ал. 1 от закона, и привеждат устройствените правилници за дейността на администрациите си в съответствие със закона.

В настоящия Устройствен правилник на Министерството на здравеопазването (УПМЗ) не са отразени новите правомощия на министъра на здравеопазването, регламентирани с Решение № 192 на Министерския съвет от 2019 г. за определяне на административните органи, към които се създават национални компетентни органи по мрежова и информационна сигурност, и за приемане на Методика за определяне на оператори на съществени услуги в съответствие с изискванията на Закона за киберсигурност.

1.2. Опишете какви са проблемите в прилагането на съществуващото законодателство или възникналите обстоятелства, които налагат приемането на ново законодателство. Посочете възможно ли е проблемът да се реши в рамките на съществуващото законодателство чрез промяна в организацията на работа и/или чрез въвеждане на нови технологични възможности (например съвместни инспекции между няколко органа и др.).

Определянето на административен орган, към който се създава национален компетентен орган по мрежова и информационна сигурност за сектор „Здравеопазване“ е изцяло нова дейност за Министерството на здравеопазването, поради което идентифицираният проблем не е възможно да бъде решен в рамките на съществуващото законодателство, чрез промяна в организацията на работа и/или чрез въвеждане на нови технологични възможности.

1.3. Посочете дали са извършени последващи оценки на нормативния акт, или анализи за изпълнението на политиката и какви са резултатите от тях?

Не са извършвани последващи оценки на въздействието на проекта на нормативен акт.

2. Цели:

Посочете целите, които си поставя нормативната промяна, по конкретен и измерим начин и график, ако е приложимо, за тяхното постигане. Съответстват ли целите на действащата стратегическа рамка?

С проекта на акт се цели да се:

- осигури съответствие на УПМЗ с Решение № 192 на Министерския съвет от 2019 г. за определяне на административните органи, към които се създават национални компетентни органи по мрежова и информационна сигурност, и за приемане на Методика за определяне на оператори на съществени услуги в съответствие с изискванията на Закона за киберсигурност;
- допълнят правомощията на министъра на здравеопазването, свързани с определянето му за административен орган, към който се създава национален компетентен орган по мрежова и информационна сигурност за сектор „Здравеопазване“;
- осигури изпълнението на новите функции на Министерството на здравеопазването, свързани с определянето на министъра на здравеопазването за административен орган, към който се създава национален компетентен орган по мрежова и информационна

сигурност за сектор „Здравеопазване“;

- допълни функционалната компетентност на звено „Сигурност на информацията и защита на данните“ в съответствие с Решение № 192 на Министерския съвет от 2019 г. за определяне на административните органи, към които се създават национални компетентни органи по мрежова и информационна сигурност, и за приемане на Методика за определяне на оператори на съществени услуги в съответствие с изискванията на Закона за киберсигурност.

Предложеният проект на постановление е съобразен с включената в управленската програма на правителството към Приоритет 64 „Развитие на електронното управление като основа за модернизация на държавната администрация и оптимизиране на процесите по административно обслужване на гражданите и бизнеса“ мярка 884 „Осигуряване на мрежова и информационна сигурност“.

3. Идентифициране на заинтересованите страни:

Посочете всички потенциални засегнати и заинтересовани страни, върху които предложението ще окаже пряко или косвено въздействие (бизнес в дадена област/всички предприемачи, неправителствени организации, граждани/техни представители, държавни органи, др.).

- администрацията на Министерството на здравеопазването;
- здравните заведения по чл. 21, ал. 2 и 3 от Закона за здравето и лечебните заведения по чл. 5, 8, 9 и 10 от Закона за лечебните заведения;
- потребителите на услуги в областта на здравни, здравно-консултативни и лечебни дейности и спешна медицинска помощ.

4. Варианти на действие:

Идентифицирайте основните регулаторни и нерегулаторни възможни варианти на действие от страна на държавата, включително варианта „Без действие“.

По своята същност УПМЗ не въвежда норми за регулиране на стопански субекти, а урежда въпросите, свързани с определяне на организационните структури на Министерството на здравеопазването, функциите, числеността на персонала и организацията на работа. Поради това при този нормативен акт могат да бъдат формулирани два варианта за действие: вариант „Без действие“ и вариант „Приемане на предлаганата промяна“.

Вариант 1 „Без действие“:

В случай, че не бъде приет проектът на Постановление на Министерския съвет за изменение и допълнение на УПМЗ, това ще доведе до несъответствие между Решение № 192 на Министерския съвет от 2019 г. за определяне на административните органи, към които се създават национални компетентни органи по мрежова и информационна сигурност, и за приемане на Методика за определяне на оператори на съществени услуги в съответствие с изискванията на Закона за киберсигурност и УПМЗ.

В случай, че не бъде прието изменение и допълнение на УПМЗ, няма да бъдат отразени новите функции на министъра на здравеопазването и няма да бъде определено структурно звено в администрацията на Министерството на здравеопазването, на което да бъдат възложени функциите по Решение № 192 на Министерския съвет от 2019 г., което да подпомага министъра на здравеопазването и да изпълнява функциите на национален компетентен орган по мрежова и информационна сигурност за сектор „Здравеопазване“.

Вариант 2 „Приемане на предлаганата промяна“:

При този вариант ще се постигне съответствие между Решение № 192 на Министерския съвет от 2019 г. и УПМЗ и ще се осигури изпълнението на новите функции и отговорности на Министерството на здравеопазването, свързани с определянето на министъра на здравеопазването за административен орган, към който се създава национален компетентен орган по мрежова и информационна сигурност за сектор „Здравеопазване“.

С проекта на Постановление на Министерския съвет за изменение и допълнение на УПМЗ се допълват разпоредбите, регламентиращи правомощията на министъра на здравеопазването, във връзка с определянето му за административен орган, към който се създава национален компетентен орган по мрежова и информационна сигурност за сектор „Здравеопазване“, а също така се допълва и функционалната компетентност на звено „Сигурност на информацията и защита на данните“. Звеното ще изпълнява функциите на национален компетентен орган по мрежова и информационна сигурност за сектор „Здравеопазване“ и на секторен екип за реагиране при инциденти с компютърната сигурност за сектор „Здравеопазване“.

5. Негативни въздействия:

Опишете качествено (при възможност – и количествено) всички значителни потенциални икономически, социални, екологични и други негативни въздействия за всеки един от вариантите, в т.ч. разходи (негативни въздействия) за идентифицираните заинтересовани страни в резултат на предприемане на действията. Пояснете кои разходи (негативни въздействия) се очаква да бъдат второстепенни и кои да са значителни.

Вариант 1 „Без действие“:

При този вариант няма да се постигне съответствие между Решение № 192 на Министерския съвет от 2019 г., Закона за киберсигурност и УПМЗ.

Този вариант ще доведе до невъзможност за изпълнение на изискването за създаване на национален компетентен орган по мрежова и информационна сигурност за сектор „Здравеопазване“ към министъра на здравеопазването.

В условията на нарастваща и необратима дигитална зависимост липсата на координация и взаимодействие между административните органи, операторите на съществени услуги и доставчиците на цифрови услуги в ключовия сектор „Здравеопазване“ ще доведат до дефицити в мрежовата и информационната сигурност и компрометиране на основни услуги, спиране на дейности и загуби.

Вариант 2 „Приемане на предлаганата промяна“:

При този вариант не се идентифицират негативни въздействия за заинтересованите страни.

6. Положителни въздействия:

Опишете качествено (при възможност – и количествено) всички значителни потенциални икономически, социални, екологични и други ползи за идентифицираните заинтересовани страни за всеки един от вариантите в резултат на предприемане на действията. Посочете как очакваните ползи кореспондират с формулираните цели.

Вариант 1 „Без действие“:

При този вариант не се идентифицират положителни въздействия за заинтересованите страни.

Вариант 2 „Приемане на предлаганата промяна“:

Приемането на промени в УПМЗ ще позволи успешното изпълнение на правомощията на министъра на здравеопазването и функциите на Министерството на здравеопазването, свързани с определянето му за административен орган, към който се създава национален компетентен орган по мрежова и информационна сигурност за сектор „Здравеопазване“.

Ще се повиши нивото на защита срещу инциденти, рискове и заплахи за мрежовата и информационната сигурност в сектор „Здравеопазване“ чрез създаване на подготвеност и работещо сътрудничество за адекватна реакция и бърз отговор в случай на киберинциденти.

По-високото ниво на сигурност ще подобри доверието на гражданите в онлайн средата и те ще могат изцяло да се възползват от възможностите на цифровия свят, в т.ч. и от електронно здравеопазване.

7. Потенциални рискове:

Посочете възможните рискове от приемането на нормативната промяна, включително възникване на съдебни спорове.

Не се идентифицират потенциални рискове от приемането на предлаганата промяна.

8.1. Административната тежест за физическите и юридическите лица:

- Ще се повиши
- Ще се намали
- Няма ефект

8.2. Създават ли се нови регулаторни режими? Засягат ли се съществуващи режими и услуги?

Не се създават нови и не се засягат съществуващи регулаторни режими.

9. Създават ли се нови регистри?

Когато отговорът е "да", посочете колко и кои са те.

Не се създават нови регистри.

10. Как въздейства актът върху микро-, малките и средните предприятия (МСП)?

- Актът засяга пряко МСП
- Актът не засяга МСП
- Няма ефект

11. Проектът на нормативен акт изисква ли цялостна оценка на въздействието?

- Да
- Не

12. Обществени консултации:

Съгласно чл. 26, ал. 3 и 4 от Закона за нормативните актове проектът на Постановление на Министерския съвет за изменение и допълнение на УПМЗ заедно с доклада и предварителната частична оценка на въздействието ще бъдат публикувани за обществено обсъждане на Портала за обществени консултации и на интернет страницата на Министерството на здравеопазването, за срок от 30 дни. Справката за постъпилите предложения заедно с обосновка за неприетите предложения ще бъде публикувана на Портала за обществени консултации и на интернет страницата на Министерството на здравеопазването.

Проектът на Постановление на Министерския съвет за изменение и допълнение на УПМЗ

ще се съгласува в съответствие с чл. 32, ал. 1 от Устройствения правилник на Министерския съвет и на неговата администрация с останалите министри.

Обобщете най-важните въпроси за консултации в случай на извършване на цялостна оценка на въздействието или за обществените консултации по чл. 26 от Закона за нормативните актове. Посочете индикативен график за тяхното провеждане и видовете консултационни процедури.

13. Приемането на нормативния акт произтича ли от правото на Европейския съюз?

Да

Не

Моля посочете изискванията на правото на Европейския съюз, включително информацията по т. 8.1 и 8.2, дали е извършена оценка на въздействието на ниво Европейски съюз, и я приложете (или посочете връзка към източник).

14. Име, длъжност, дата и подпис на директора на дирекцията, отговорна за изработването на нормативния акт:

Име и длъжност: Христина Гетова, директор на дирекция „Правна“

Дата:

Подпис: