Частична предварителна оценка на въздействието	
Институция: Министерство на вътрешните работи	**Нормативен акт:** Закон за Министерството на вътрешните работи (ЗМВР)
◉ Не е включен в законодателна/оперативна програма на Министерския съвет	○ Включен е в законодателната/оперативната програма на Министерския съвет за: ……
Лице за контакт: Нина Василева Чимова Пенка Ценова -Христова	**Телефон и ел. поща:** 982 2931 pravna@mvr.bg

1. Проблем/проблеми за решаване:

Проблем 1. „ Оправомощаване на полицейските органи да извършват справки в Общото хранилище с данни за самоличност (ОХДС) на ЕС с цел установяване на самоличност на граждани на трети страни“.

С Регламент (ЕС) 2019/817 и Регламент (ЕС) 2019/818 на Европейския парламент и на Съвета от 20 май 2019 година е създадена рамка за оперативна съвместимост между информационните системи на ЕС в областта на границите, визите, полицейското и съдебното сътрудничество, убежището и миграцията (ОВ L 135, 22.5.2019 г.)

Компонентите на опретавинта съвместимост обхващат Системата за влизане/излизане (СВИ), Визовата информационна система (ВИС), Европейската система за информация за пътуванията и разрешаването им (ETIAS), Евродак, Шенгенската информационна система (ШИС) и Европейската информационна система за съдимост за граждани на трети държави (ECRIS-TCN). За постигането на тази функционалност на информационните системи като компоненти на оперативната съвместимост са предвидени: европейски портал за търсене (ЕПТ), обща услуга за биометрично съпоставяне (обща УБС), общо хранилище на данни за самоличност (ОХДС) и детектор за множество самоличности ДМС.

СВИ, ВИС, ETIAS, Евродак и ECRIS-TCN изискват точното установяване на самоличността на лицата, чиито данни са регистрирани в тях. Въпреки това е възможно личните данни, съхранявани в отделните информационни системи, да се отнасят за едни и същи лица, но да са под различна или непълна самоличност. ОХДС следва да улеснява правилното установяване на самоличността на лицата, независимо от системата, в която данните за тяхната самоличност, данните от документа за пътуване и биометрични данни са били събрани първоначално.

За улесняване на проверките за установяване на самоличността на добросъвестните пътници и за борба срещу използването на фалшива самоличност в ОХДС се създава лично досие, с държащо

цялата обобщена информация на едно място.
Когато полицейски орган на държава членка не е в състояние да установи самоличността на дадено лице, поради липса на документ за пътуване или друг достоверен документ, доказващ самоличността на това лице, или когато са налице съмнения относно данните за самоличност, предоставени от това лице, или относно автентичността на документа за пътуване или самоличността на неговия притежател, или когато лицето не е в състояние или отказва да сътрудничи, този полицейски орган следва да може да извърши търсене в ОХДС, за да установи самоличността на лицето. За тези цели полицейските органи следва да снемат пръстови отпечатъци чрез използване на директно сканиращи устройства за снемане на пръстови отпечатъци, при условие че процедурата е започнала в присъствието на лицето.
За да се възползват от посочената опция и да имат право полицейските служители да достъпват ОХДС чрез Европейския портал за търсене, държавите членки следва да приемат национални законодателни мерки, с които да определят органите, компетентни да извършват проверки за установяване на самоличността на граждани на трети страни като използват ОХДС, да уредят процедурите, условията и критериите за тези проверки, при които следва да се спазва принципът на пропорционалност.

Проблем 2. „Осигуряване на прилагането на Регламент (ЕС) 2021/784 на Европейския парламент и на Съвета от 29 април 2021 година относно справянето с разпространението на терористично съдържание онлайн (ОВ L 172, 17.5.2021 г.) “

С регламента се установяват единни правила за справяне със злоупотребата с хостинг услуги за разпространение на терористично съдържание онлайн.
Регламентът е приет в отговор на нарастващия брой злоупотреби с услугите, предлагани от доставчиците на хостинг, от страна на терористични групи и на техните поддръжници, за да разпространяват терористично съдържание онлайн, с цел отправяне на техните послания, радикализиране и вербуване на последователи, както и улесняване и ръководене на терористична дейност. Наличието на терористично съдържание онлайн се оказва катализатор за радикализацията на лица, която може да доведе до терористични актове, и следователно има сериозни отрицателни последици за ползвателите, гражданите и обществото като цяло.
Регламентът се прилага за доставчиците на хостинг услуги, които предлагат услуги в Съюза, независимо от тяхното основно място на стопанска дейност. Въвежда се задължение за доставчиците на хостинг услуги за бързото премахване или блокиране на достъпа до терористично съдържание. В същото време налаганите мерки следва да бъдат необходими, подходящи и пропорционални в едно демократично общество, като не се засягат основните принципи, свързани със свободата на изразяване на мнение и свободата на информация, включително свободата и плурализма на медиите.
Необходимо е да се осигури прилагането в българската нормативна уредба на основни елементи от Регламент (ЕС) 2021/784, като: определянето на компетентни национални органи съгласно чл. 12, които могат да издават заповед за премахване, с която от доставчика на хостинг услуги се изисква да премахне терористично съдържание или да блокира достъпа до терористично съдържание във всички държави членки, да следят за прилагането на конкретни мерки от доставчиците, изложени на терористично съдържание, както и да налагат санкции за доставчици на хостинг услуги при системно или трайно неспазване на задълженията им, съгласно чл. 18 от регламента.
Компетентните национални органи следва да изготвят годишни доклади за прозрачност,

съдържащи информация относно броя на заповедите за премахване, броя на случаите, в които не е била изпълнена заповед, броя на решенията относно конкретните мерки, броя на случаите, които са обжалвани по административен или съдебен ред и броя на решенията за налагане на санкции.

Проблемите не могат да бъдат решени в рамките на съществуващата нормативна уредба или чрез промяна в организацията на работа и /или въвеждане на нови технологични възможности, предвид че правилата, въведени с регламентите са нови и предполагат установяване на законово ниво на необходимите предпоставки за изпълнение чрез определяне на компетентните органи, които да прилагат съответните правомощия и процедури.

Не е извършвана последваща оценка на въздействието на Закона за Министерството на вътрешните работи.

2. Цели:

Цел 1: „ Използване на оперативната съвместимост между информационните системи на ЕС за подобряване на контрола по външните граници, предотвратяване на незаконната миграция, противодействието на терористични и други тежки престъпления, поддържане на обществения ред и сигурност **“.**

Цел 2: „ Гарантиране на безпрепятственото функциониране на цифровия единен пазар чрез справяне с разспространението на терористичното съдържание онлайн. **“.**

3. Заинтересовани страни:

1. По проблем 1:

Полицейските органи на Министерството на вътрешните работи:

Главна дирекция "Национална полиция", Главна дирекция "Борба с организираната престъпност", Главна дирекция "Жандармерия, специални операции и борба с тероризма", Главна дирекция "Гранична полиция", областните дирекции, дирекция "Миграция", дирекция "Вътрешна сигурност", дирекция "Международно оперативно сътрудничество

Граждани на трети страни при преминаване на границите и пребиваване на територията на страната.

2. По проблем 2:

Главна дирекция „Борба с организираната престъпност“ - МВР;

Хостинг компании, осъществяващи дейност на територията на страната и в ЕС.

4. Варианти на действие. Анализ на въздействията:

4.1. По проблем 1:

Вариант 1 „Без действие“:

Описание: Няма да се приемат национални законодателни мерки, с които да се определят органите, компетентни да извършват проверки за установяване на самоличността като използват ОХДС и няма да се уреждат процедурите, условията и критериите за тези проверки.

Положителни (икономически/социални/екологични) въздействия:

Не се очакват.

Отрицателни (икономически/социални/екологични) въздействия:

Полицейските органи няма да разполагат с правомощието да извършват справки в ОХДС с цел установяване на самоличността на лица. Създадената технологична възможност чрез оперативна съвместимост между информационните системи на ЕС ще остане неприложима за националните правоприлагащи органи, които няма да могат да извършват търсене и справки с базите данни.

Специфични въздействия:

Въздействия върху малките и средните предприятия: Няма

Административна тежест: Не се предвижда. Нормативните промени няма да доведат до установяване на нови или изменение на съществуващи регулаторни режими.

Вариант 2 „Предприемане на нормативни изменения“:

Описание:

В Закона за МВР ще бъде разписано правомощието на полицейските органи да установяват самоличност чрез използване на ОХДС. Търсенията в ОХДС ще се извършват от полицейски орган в съответствие с Регламент (ЕС) 2019/817 и Регламент (ЕС) 2019/818 на Европейския парламент и на Съвета от 20 май 2019 година в случаите, когато полицейският орган не е в състояние да установи самоличността на дадено лице поради липсата на документ за пътуване или друг достоверен документ, когато има съмнения относно данните за самоличност, предоставени от дадено лице или относно автентичността на документа за пътуване или друг достоверен документ, предоставен от дадено лице или когато дадено лице не е в състояние или отказва да сътрудничи.

Положителни (икономически/социални/екологични) въздействия:
Биометричните данни, като пръстови отпечатъци и портретни снимки, са единствени по рода си и поради това са много по-надеждни за целите на установяване на самоличността на дадено лице от буквено-цифровите данни. Ще може да се използва общата услуга за биометрично съпоставяне като техническо средство за подсилване и улесняване на работата на съответните информационни системи на ЕС и на другите компоненти за оперативна съвместимост. По този начин ще бъде улеснено установяването на самоличността на физическо лице, което е регистрирано в няколко бази данни, чрез използването на един-единствен технологичен компонент за съпоставяне на биометричните данни на това физическо лице в различните системи, вместо на няколко различни компонента. Това ще доведе до по-голяма сигурност и надеждност на проверките.

Отрицателни (икономически/социални/екологични) въздействия:

Не се очакват.

Специфични въздействия:

Въздействия върху малките и средните предприятия: Няма

Административна тежест: Не се предвижда. Нормативните промени няма да доведат до установяване на нови или изменение на съществуващи регулаторни режими

4.2. По проблем 2:

Вариант 1 „Без действие“:

Описание: Няма да се осигури прилагането в българската нормативна уредба на основни елементи от Регламент (ЕС) 2021/784.

Положителни (икономически/социални/екологични) въздействия:

Не се очакват.

Отрицателни (икономически/социални/екологични) въздействия:

Няма да бъдат определени компетентни национални органи съгласно чл. 12 от регламента, които могат да издават заповед за премахване, с която от доставчика на хостинг услуги се изисква да премахне терористично съдържание или да блокира достъпа до терористично съдържание във всички държави членки. Няма да се дефинирани компетентните национални органи, които да следят за прилагането на конкретни мерки от доставчиците, изложени на терористично съдържание, да налагат санкции за доставчици на хостинг услуги при системно или трайно неспазване на задълженията им съгласно чл. 18 от регламента, както и да изготвят годишни доклади за прозрачност, съдържащи информация относно броя на заповедите за премахване, броя на случаите, в които не е била изпълнена заповед, броя на решенията относно конкретните мерки, броя на случаите, които са обжалвани по административен или съдебен ред и броя на решенията за налагане на санкции.

Специфични въздействия:

Въздействия върху малките и средните предприятия: Няма

Административна тежест: Няма

Вариант 2 „Предприемане на нормативни изменения“:

Описание: В националното законодателство ще се осигури прилагането в на основните елементи от Регламент (ЕС) 2021/784, като ще бъдат определени компетентни национални органи съгласно чл. 12, които могат да издават заповед за премахване, с която от доставчика на хостинг услуги се изисква да премахне терористично съдържание или да блокира достъпа до терористично съдържание във всички държави членки, да следят за прилагането на конкретни мерки от доставчиците, изложени на терористично съдържание, както и да налагат санкции за доставчици на хостинг услуги при системно или трайно неспазване на задълженията им, съгласно чл. 18 от регламента.

Ще се определят и приложимите национални процедури за обжалване от страна на засегнатите оператори – доставчици на хостинг услуги, както и реда за изготвяне на годишни доклади за прозрачност, съдържащи информация относно броя на заповедите за премахване, броя на

случаите, в които не е била изпълнена заповед, броя на решенията относно конкретните мерки, броя на случаите, които са обжалвани по административен или съдебен ред и броя на решенията за налагане на санкции.

Положителни (икономически/социални/екологични) въздействия:

От компетентните национални органи ще се прилагат единни правила за справяне със злоупотребата с хостинг услуги за разпространение сред обществеността на терористично съдържание онлайн, по-специално, свързани с разумни и пропорционални задължения на доставчиците на хостинг услуги за полагане на дължима грижа с цел справяне с разпространението сред обществеността на терористично съдържание чрез техните услуги и за да се гарантира, когато е необходимо, бързото му премахване или блокиране на достъпа до такова съдържание.

Отрицателни (икономически/социални/екологични) въздействия: Не се очакват.

Специфични въздействия:

Въздействия върху малките и средните предприятия: от доставчиците на хостинг услуги се ще се изисква да премахнат терористично съдържание или да блокират достъпа до терористично съдържание във всички държави членки.
Доставчик на хостинг услуги, който е изложен на терористично съдържание ще следва да предприеме конкретни мерки за защита на своите услуги срещу разпространението на терористично съдържание сред обществеността. Такива мерки могат да бъдат подходящи технически и оперативни мерки или способности, например подходящ персонал или технически средства за идентифициране и бързо премахване или блокиране на достъпа до терористично съдържание; леснодостъпни и лесни за ползване механизми, чрез които ползвателите да съобщават или сигнализират на доставчика на хостинг услуги за предполагаемо терористично съдържание; всякакви други механизми за повишаване на осведомеността за наличието на терористично съдържание в неговите услуги, например механизми за модериране на ползвателите или всяка друга мярка, която доставчикът на хостинг услуги смята за подходяща за справяне с наличието на терористично съдържание в своите услуги.
Доставчиците на хостинг услуги ще могат да обжалват по административен и съдебен ред наложените ограничения.
Административна тежест: Следва да се установят правилата относно санкциите, приложими при нарушения на Регламент (ЕС) 2021/784. Санкциите трябва да бъдат ефективни, пропорционални и възпиращи. При вземането на решение дали да бъде наложена санкция и при определянето на вида и тежестта на санкциите компетентните органи следва да вземат предвид всички значими обстоятелства, включително: естеството, тежестта и продължителността на нарушението; дали нарушението е било умишлено или е било резултат от небрежност; предишни нарушения, извършени от доставчика на хостинг услуги; финансовото състояние на доставчика на хостинг услуги; степента на съдействие на доставчика на хостинг услуги с компетентните органи; естеството и размера на доставчика на хостинг услуги, по-специално дали той е микро-, малко или средно предприятие; степента на вина на доставчика на хостинг услуги, като се вземат предвид техническите и организационните мерки, предприети от него за изпълнение на настоящия регламент.
Системното или трайно неспазване на задълженията на доставчиците на хостинг услуги следва да подлежи на финансова санкция в размер до 4 % от общия оборот на доставчика на хостинг

услуги за предишната финансова година.

5. Сравняване на вариантите:

Степени на изпълнение по критерии: 1) висока; 2) средна; 3) ниска.

5.1. По проблем 1:

		Вариант „Без действие“	**Вариант 1**
Ефективност	Цел 1: Използване на оперативната съвместимост между информационните системи на ЕС за подобряване на контрола по външните граници, предотвратяване на незаконната миграция, противодействието на терористични и други тежки престъпления, поддържане на обществения ред и сигурност **“**	3	1
Ефикасност	Цел 1: Използване на оперативната съвместимост между информационните системи на ЕС за подобряване на контрола по външните граници, предотвратяване на незаконната миграция,	3	1

	противодействието на терористични и други тежки престъпления, поддържане на обществения ред и сигурност “		
Съгласуваност	Цел 1: Използване на оперативната съвместимост между информационните системи на ЕС за подобряване на контрола по външните граници, предотвратяване на незаконната миграция, противодействието на терористични и други тежки престъпления, поддържане на обществения ред и сигурност “	3	1

5.2. По проблем 2:

		Вариант „Без действие“	**Вариант 1**
Ефективност	Цел 2: „ Гарантиране на безпрепятственото функциониране на цифровия единен пазар чрез справяне с разспространението	3	1

	на терористичното съдържание онлайн. “			
Ефикасност	Цел 2: „ Гарантиране на безпрепятственото функциониране на цифровия единен пазар чрез справяне с разспространението на терористичното съдържание онлайн. “	З	1	
Съгласуваност	Цел 1: „ Гарантиране на безпрепятственото функциониране на цифровия единен пазар чрез справяне с разспространението на терористичното съдържание онлайн. “	3	1	

6. Избор на препоръчителен вариант:

По проблем 1: Вариант 2 „Предприемане на нормативни изменения “

По проблем 2: Вариант 2 „Предприемане на нормативни изменения“

6.1. Промяна в административната тежест за физическите и юридическите лица от прилагането на препоръчителния вариант (включително по отделните проблеми):

- (•) Ще се увеличи
- ( ) Ще се намали
- ( ) Няма ефект

Следва да се установят правилата относно санкциите, приложими при нарушения на Регламент (ЕС) 2021/784.Санкциите трябва да бъдат ефективни, пропорционални и възпиращи. При вземането на решение дали да бъде наложена санкция и при определянето на вида и тежестта на

санкциите компетентните органи следва да вземат предвид всички значими обстоятелства, включително: естеството, тежестта и продължителността на нарушението; дали нарушението е било умишлено или е било резултат от небрежност; предишни нарушения, извършени от доставчика на хостинг услуги; финансовото състояние на доставчика на хостинг услуги; степента на съдействие на доставчика на хостинг услуги с компетентните органи; естеството и размера на доставчика на хостинг услуги, по-специално дали той е микро-, малко или средно предприятие; степента на вина на доставчика на хостинг услуги, като се вземат предвид техническите и организационните мерки, предприети от него за изпълнение на настоящия регламент.
Системното или трайно неспазване на задълженията на доставчиците на хостинг услуги следва да подлежи на финансова санкция в размер до 4 % от общия оборот на доставчика на хостинг услуги за предишната финансова година.

6.2. Създават ли се нови/засягат ли се съществуващи регулаторни режими и услуги от прилагането на препоръчителния вариант (включително по отделните проблеми)?

○ Да

……..……
…….

◉ Не

6.3. Създават ли се нови регистри от прилагането на препоръчителния вариант (включително по отделните проблеми)?

○ Да

……..……
…….

◉ Не

Когато отговорът е „Да“, посочете регистрите, които се създават и по какъв начин те ще бъдат интегрирани в общата регистрова инфраструктура.

6.4. По какъв начин препоръчителният вариант въздейства върху микро-, малките и средните предприятия (МСП) (включително по отделните проблеми)?

◉ Актът засяга пряко МСП

○ Актът не засяга МСП

6.5. Потенциални рискове от прилагането на препоръчителния вариант (включително по отделните проблеми):

Не се идентифицират.

7. Консултации:

○ Проведени са консултации

……..……
……..
……..

Посочете основните заинтересовани страни, с които са проведени консултации. Посочете резултатите от консултациите, включително на ниво ЕС: спорни въпроси, многократно поставяни въпроси и др.

◉ Предстоят обществени консултации по чл. 26 от Закона за нормативните актове

……..……
……..
……..

Обобщете най-важните въпроси за обществени консултации. Посочете индикативен график за тяхното провеждане и видовете консултационни процедури.

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

◉ Да

○ Не

Регламент (ЕС) 2019/817 и Регламент (ЕС) 2019/818 на Европейския парламент и на Съвета от 20 май 2019 година за създаване, Регламент (ЕС) 2021/784 на Европейския парламент и на Съвета от 29 април 2021 година относно справянето с разпространението на терористично съдържание онлайн

9. Изисква ли се извършване на цялостна предварителна оценка на въздействието поради очаквани значителни последици?

○ Да

◉ Не

(преценка съгласно чл. 20, ал. 3, т. 2 от Закона за нормативните актове)

10. Приложения:

……..……
……

Приложете необходимата допълнителна информация и документи.

11. Информационни източници:

……..……
……

Посочете изчерпателен списък на информационните източници, които са послужили за оценка на въздействията на отделните варианти и при избора на вариант за действие: регистри, бази данни, аналитични материали и др.

12. Име, длъжност, дата и подпис на директора на дирекцията, отговорна за извършването на частичната предварителна оценка на въздействието:

Име и длъжност: Александър Стефанов ВПД директор на дирекция „Правно-нормативна дейност“

Дата: 23.01.2023 г.

Подпис: /п/