ПРЕПОРЪКИ

ПРЕПОРЪКА (ЕС) 2019/534 НА КОМИСИЯТА

от 26 март 2019 година

Киберсигурност на 5G мрежите

ЕВРОПЕЙСКАТА КОМИСИЯ,

като взе предвид Договора за функционирането на Европейския съюз, и по-специално член 292 от него,

като има предвид, че:

(1) Комисията разглежда разгръщането на мрежовите технологии от 5-то поколение (5G) като важен фактор за предоставянето на цифрови услуги в бъдеще и приоритет в стратегията за цифров единен пазар. Комисията прие план за действие за 5G с цел Съюзът да разполага с инфраструктура за свързаност, необходима за неговата цифровата трансформация от 2020 г. нататък ([1]).

(2) 5G мрежите ще се основават на настоящите мрежови технологии от 4-то поколение (4G), като ще осигурят нови възможности за предоставяне на услуги и ще се превърнат в централната инфраструктура и фактор за развитието на големи части от икономиката на Съюза. След разгръщането на 5G мрежите те ще образуват гръбнака на широк набор от услуги, които са от съществено значение за функционирането на вътрешния пазар и за поддръжката и осъществяването на жизненоважни обществени и икономически функции, като например енергетиката, транспорта, банковото дело и здравеопазването, както и системите за промишлен контрол. Организацията на демократичните процеси, например избори, също все повече ще зависи от цифровата инфраструктура и 5G мрежите.

(3) Тъй като множество критични услуги са зависими от 5G мрежите, последиците от системни и широкоразпространени смущения ще са особено сериозни. Поради това осигуряването на киберсигурността на 5G мрежите е въпрос от стратегическо значение за Съюза във време, в което кибератаките стават все по-чести и по-сложни от когато и да било.

(4) Взаимозависимостта и транснационалният характер на инфраструктурите в основата на цифровата екосистема и трансграничният характер на заплахите означават, че всички значителни уязвимости и/или киберинциденти, свързани с 5G мрежите в една държава членка, ще засегнат целия Съюз. Затова трябва да се предприемат мерки за осигуряване на високо общо ниво на киберсигурност на 5G мрежите.

(5) Необходимостта от действия на равнището на Съюза бе потвърдена от държавите членки. В своите заключения от 21 март 2019 г. Европейският съвет посочва, че очаква препоръка на Комисията относно съгласуван подход към сигурността на 5G мрежите ([2]).

(6) Гарантирането на европейския суверенитет следва да бъде основна цел при пълно зачитане на европейските ценности отвореност и толерантност ([3]). Чуждестранните инвестиции в стратегически сектори, придобиването на критични активи, технологии и инфраструктура в Съюза и доставката на оборудване от критично значение също могат да представляват риск за сигурността на Съюза.

(7) Както се посочва в съвместното съобщение „ЕС—Китай — стратегически перспективи“ ([4]), киберсигурността на 5G мрежите е от ключово значение за гарантиране на стратегическата автономност на Съюза.

(8) В резолюцията на Европейския парламент относно заплахите за сигурността във връзка със засилващото се технологично присъствие на Китай в Съюза също се призовават Комисията и държавите членки да предприемат действия на равнището на Съюза ([5]).

(9) В настоящата препоръка се разглеждат рисковете за киберсигурността на 5G мрежите, като се определят насоки за подходящите мерки за анализ и управление на риска на национално равнище, за извършване на координирана европейска оценка и за установяване на процедура за разработване на общ инструментариум, съдържащ най-добрите мерки за управление на риска.

(10) Съществува стабилна правна уредба на Съюза за защита на електронните съобщителни мрежи.

([1]) COM(2016) 588 final.
([2]) Заключения на Европейския съвет от 21 и 22 март 2019 г.
([3]) Състояние на Съюза 2018 г. — Време за европейски суверенитет, 12 септември 2018 г.
([4]) JOIN (2019) 5 final.
([5]) www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+TA+P8-TA-2019-0156+0+DOC+PDF+V0//EN

(11) С регулаторната рамка на Съюза в областта на електронните комуникации ([6]) се насърчават конкуренцията, вътрешният пазар и интересите на крайните ползватели, а с Европейския кодекс за електронните съобщения ([7]) се преследва допълнителна цел за свързаност, изразена в резултати: широко разпространение и използване на фиксирани и мобилни мрежи с много голям капацитет за всички граждани и предприятия в Съюза, като в същото време се защитават интересите на гражданите. В Директива 2002/21/ЕО от държавите членки се изисква да гарантират поддържането на целостта и сигурността на обществените съобщителни мрежи, като са предвидени задължения за гарантиране, че предприятията, предоставящи обществени съобщителни мрежи или обществено достъпни електронни съобщителни услуги, предприемат технически и организационни мерки за подходящо управление на рисковете за сигурността на мрежите и услугите. Съгласно Директивата компетентните национални регулаторни органи трябва да разполагат с правомощия, включително правомощие за издаване на задължителни указания, за да се осигури спазването на тези задължения.

(12) Освен това Директива 2002/20/ЕО на Европейския парламент и на Съвета ([8]) позволява на държавите членки да добавят условия относно защитата на обществените мрежи срещу неразрешен достъп към общото разрешение с цел защита на поверителността на комуникациите в съответствие с Директива 2002/58/ЕО на Европейския парламент и на Съвета ([9]).

(13) С цел подпомагане на изпълнението на тези задължения Съюзът създаде редица органи за сътрудничество. Агенцията за мрежова и информационна сигурност (ENISA), Комисията, държавите членки и националните регулаторни органи разработиха технически насоки за националните регулаторни органи относно докладването на инциденти, мерките за сигурност и заплахите и активите ([10]). С Директива (ЕС) 2016/1148 на Европейския парламент и на Съвета ([11]) бе създадена група за сътрудничество („групата за сътрудничество“), в която участват компетентните органи, с цел подкрепа и улесняване на сътрудничеството, по-специално чрез предоставяне на стратегически насоки за дейностите на мрежата от екипи за реагиране при инциденти с компютърната сигурност, които улесняват оперативното сътрудничество на техническо ниво.

(14) Бъдещата европейска рамка за сертифициране на киберсигурността ([12]) следва да осигури важен помощен инструмент за насърчаване на последователност по отношение на равнищата на сигурност. Тя следва да даде възможност за разработване на схеми за сертифициране на киберсигурността с цел посрещане на нуждите на ползвателите на оборудване и софтуер, свързани с 5G мрежите. Поради критичното значение на тези инфраструктури разработването на съответните европейски схеми за сертифициране на киберсигурността на информационните и комуникационните продукти, услуги или процеси, използвани за 5G мрежите, следва да бъде непосредствен приоритет. Държавите членки и участниците на пазара следва активно да участват в разработването на такива схеми за сертифициране, включително като предоставят подкрепа за определянето на специфичните профили на защита за 5G мрежите.

(15) При липсата на хармонизирано законодателство на Съюза държавите членки могат да постановят посредством национални технически правила, приети в съответствие с правото на Съюза, че участието в дадена европейска схема за сертифициране на киберсигурността е задължително. Държавите членки могат също така да използват европейските схеми за сертифициране на киберсигурността в контекста на обществените поръчки и на Директива 2014/24/ЕС на Европейския парламент и на Съвета ([13]) и да подкрепят разработването на механизми за подпомагане — например център за подпомагане — с цел закупуване на решения за киберсигурност от страна на публичните купувачи.

(16) Наличието на високо равнище на защита на данните и неприкосновеността на личния живот е важен елемент от гарантирането на сигурността на 5G мрежите. На равнището на Съюза също така са определени правила за гарантиране на сигурността на обработването на личните данни, включително в сферата на електронните комуникации. В Общия регламент относно защитата на данните ([14]) се съдържа задължение личните данните да се обработват по начин, който гарантира тяхната сигурност, включително като се предотвратява неразрешен достъп

([6]) Директива 2002/21/ЕО на Европейския парламент и на Съвета от 7 март 2002 г. относно общата регулаторна рамка за електронните съобщителни мрежи и услуги (Рамкова директива) (ОВ L 108, 24.4.2002 г., стр. 33) и специфичните директиви.

([7]) Директива (ЕС) 2018/1972 на Европейския парламент и на Съвета от 11 декември 2018 г. за установяване на Европейски кодекс за електронни съобщения (ОВ L 321, 17.12.2018 г., стр. 36).

([8]) Директива 2002/20/ЕО на Европейския парламент и на Съвета от 7 март 2002 г. относно разрешението на електронните съобщителни мрежи и услуги (Директива за разрешение) (ОВ L 108, 24.4.2002 г., стр. 21).

([9]) Директива 2002/58/ЕО на Европейския парламент и на Съвета от 12 юли 2002 г. относно обработката на лични данни и защита на правото на неприкосновеност на личния живот в сектора на електронните комуникации (Директива за правото на неприкосновеност на личния живот и електронни комуникации) (ОВ L 201, 31.7.2002 г., стр. 37).

([10]) https://resilience.enisa.europa.eu/article-13.

([11]) Директива (ЕС) 2016/1148 на Европейския парламент и на Съвета от 6 юли 2016 г. относно мерки за високо общо ниво на сигурност на мрежите и информационните системи в Съюза (ОВ L 194, 19.7.2016 г., стр. 1).

([12]) Предложение за Регламент на Европейския парламент и на Съвета относно ENISA — Агенцията на ЕС за киберсигурност, и за отмяна на Регламент (ЕС) № 526/2013, както и относно сертифицирането на киберсигурността на информационните и комуникационните технологии („Акт за киберсигурността“) (COM(2017) 477 final — 2017/0225 (COD).

([13]) Директива 2014/24/ЕС на Европейския парламент и на Съвета от 26 февруари 2014 г. за обществените поръчки и за отмяна на Директива 2004/18/ЕО (ОВ L 94, 28.3.2014 г., стр. 65).

([14]) Регламент (ЕС) 2016/679 на Европейския парламент и на Съвета от 27 април 2016 г. относно защитата на физическите лица във връзка с обработването на лични данни и относно свободното движение на такива данни и за отмяна на Директива 95/46/ЕО (Общ регламент относно защитата на данните) (ОВ L 119, 4.5.2016 г., стр. 1).

или използване на личните данни и оборудването за тяхното обработване. В Директивата за правото на неприкосновеност на личния живот и електронни комуникации са определени специфични правила за защита на поверителността на комуникациите и на крайното оборудване на крайните потребители. С нея също така на доставчиците на услуги се налагат задължения да предприемат подходящи технически и организационни мерки, за да гарантират сигурността на своите услуги.

(17) Съюзът също така е приел инструмент, с който ще се защитават критичната инфраструктура и технологии, като тези, използвани в сферата на комуникациите, като се предоставя възможност на държавите членки да извършват скрининг на преки чуждестранни инвестиции на основания, свързани със сигурността или обществения ред, при което държавите членки и Комисията ще могат да обменят информация и да изразяват безпокойство във връзка с конкретни инвестиции ([15]).

(18) Понастоящем държавите членки и операторите предприемат важни подготвителни стъпки за създаването на условия за широкомащабното разгръщане на 5G мрежи. Няколко държави членки изразиха безпокойство относно потенциалните рискове за сигурността, свързани с 5G мрежите в контекста на провеждането на процедури за предоставяне на права за използване на радиочестотни ленти, определени за 5G мрежи ([16]), и проучват мерки за справяне с тези рискове.

(19) За справяне с рисковете за киберсигурността на 5G мрежите следва да се вземат предвид както техническите, така и други фактори. Техническите фактори могат да включват аспекти, свързани с уязвимости в сигурността, които могат да бъдат използвани за получаване на неразрешен достъп до информация (кибершпионаж по икономически или политически причини) или за други злонамерени цели (кибератаки с цел предизвикване на смущения в системи и данни или тяхното унищожение). Сред важните аспекти, които следва да бъдат взети под внимание, са необходимостта от защита на мрежите през целия им жизнен цикъл и необходимостта от обхващане на цялото съответно оборудване, включително по време на етапите на проектиране, разработване, възлагане, разгръщане, експлоатация и поддръжка на 5G мрежите.

(20) Сред другите фактори могат да бъдат регулаторни или други изисквания, наложени на доставчиците на информационно и комуникационно оборудване. При оценката на значението на тези фактори следва да се вземат предвид, *inter alia*, цялостният риск от влияние от страна на трета държава, по-специално по отношение на нейния режим на управление, липсата на споразумения за сътрудничество в областта на сигурността или подобни договорености относно защитата на данните между Съюза и въпросната трета държава, като например решения относно адекватното ниво на защита, или дали тази държава е страна по многостранни, международни или двустранни споразумения в областта на киберсигурността, борбата с киберпрестъпността или защитата на данните.

(21) На национално равнище следва да се извърши оценка на риска като важна стъпка от разработването на подход на Съюза към киберсигурността на 5G мрежите. Това ще помогне на държавите членки да адаптират националните мерки относно изискванията за сигурност и управлението на риска в светлината на тази оценка.

(22) Следва да се извършва координация, за да се гарантира ефективността на мерките за справяне с тези заплахи за киберсигурността — мерки, които са от съществено значение за гладкото функциониране на вътрешния пазар и за защитата на личните данни и неприкосновеността на личния живот.

(23) Националните оценки на риска следва да формират основата на координирана оценка на риска на равнището на Съюза, състояща се от установяване на картината на заплахите и съвместен преглед, който следва да се извърши от държавите членки заедно с Агенцията на Европейския съюз за киберсигурност (ENISA) и с подкрепата на Комисията.

(24) Като вземе предвид националните оценки на риска и оценката на риска на равнището на Съюза, групата за сътрудничество следва да създаде инструментариум за идентифициране на видовете рискове за киберсигурността и определяне на евентуални мерки за намаляване на рисковете в области като сертифициране, изпитване и контрол на достъпа. Тя също така следва да определи евентуални специфични мерки, подходящи за справяне с рисковете, идентифицирани от една или повече държави членки. Групата за сътрудничество следва да се ползва от подкрепата на Агенцията на Европейския съюз за киберсигурност (ENISA), Европол, Органа на европейските регулатори в областта на електронните съобщения (ОЕРЕС) и Центъра на ЕС за анализ на информация. Този инструментариум следва да послужи за консултиране на Комисията във връзка с разработването на минимални общи изисквания за гарантиране в още по-голяма степен на високо ниво на киберсигурност на 5G мрежите в целия Съюз.

(25) Когато се предприемат мерки за справяне с рисковете за киберсигурността, следва да се обърне внимание на насърчаването на киберсигурността чрез разнообразие на доставчиците при изграждането на дадена мрежа.

([15]) Регламент (ЕС) 2019/452 на Европейския парламент и на Съвета от 19 март 2019 г. за създаване на рамка за скрининг на преки чуждестранни инвестиции в Съюза (ОВ L 79I, 21.3.2019 г., стр. 1).

([16]) През 2019 г. са планирани тръжни процедури за поне една честотна лента в 11 държави членки: Австрия, Белгия, Чехия, Франция, Германия, Гърция, Унгария, Ирландия, Нидерландия, Литва, Португалия. Шест други търга са планирани за 2020 г.: Испания, Малта, Литва (различни честоти), Словакия, Полша, Обединено кралство. Източник: http://5gobservatory.eu/observatory-overview/observatory-reports/

(26) Настоящата препоръка следва да не засяга компетентността на държавите членки по отношение на дейностите, свързани с обществената сигурност, отбраната и националната сигурност, и дейностите на държавите в областта на наказателното право, включително правото на държавите членки да не допускат доставчици до своите пазари по съображения, свързани с националната сигурност,

ПРИЕ НАСТОЯЩАТА ПРЕПОРЪКА:

I. **ЦЕЛИ**

1) С цел подкрепа на разработването на подход на Съюза за гарантиране на киберсигурността на 5G мрежите в настоящата препоръка се посочват действията, които следва да бъдат предприети, за да се осигурят условия:

а) държавите членки да извършат оценка на рисковете за киберсигурността, засягащи 5G мрежите на национално равнище и да предприемат необходимите мерки за сигурност.

б) държавите членки и съответните институции, агенции и други органи на Съюза да изготвят съвместно координирана оценка на риска на равнището на Съюза, която се основава на националната оценка на риска.

в) групата за сътрудничество, създадена по силата на Директива (ЕС) 2016/1148 („групата за сътрудничество“), да определи евентуален общ набор от мерки, които да бъдат предприети с цел намаляване на рисковете за киберсигурността, свързани с инфраструктурите в основата на цифровата екосистема, по-специално 5G мрежите.

II. **ОПРЕДЕЛЕНИЯ**

2) За целите на настоящата препоръка:

а) „5G мрежи“ означава набор от всички съответни елементи на мрежовата инфраструктура за технологията на мобилна и безжична комуникация, използвани за постигане на свързаност и предоставяне на услуги с добавена стойност, имащи усъвършенствани експлоатационни характеристики, като например много висока скорост на пренос на данни и много голям капацитет, комуникации с ниска латентност и изключително висока надеждност, или поддържащи голям брой свързани устройства. Те могат да включват заварени мрежови елементи, основаващи се на предишни поколения технологии за мобилна и безжична комуникация, като например 4G или 3G. 5G мрежите следва да се разбират като включващи всички съответни части на мрежата.

б) „инфраструктури в основата на цифровата екосистема“ означава инфраструктурите, използвани, за да се осигури възможност за цифровизация на широк кръг от критични приложения в икономиката и обществото.

III. **ДЕЙСТВИЯ НА НАЦИОНАЛНО РАВНИЩЕ**

3) До 30 юни 2019 г. държавите членки следва да извършат оценка на риска за инфраструктурата за 5G мрежи, включваща идентифициране на най-чувствителните елементи, при които пробивите в сигурността ще имат значителни отрицателни последици. До същата дата държавите членки следва също така да извършат преглед на изискванията за сигурност и методите за управление на риска, приложими на национално равнище, за да вземат под внимание рисковете за киберсигурността, които могат да възникнат поради i) технически фактори, като например специфичните технически характеристики на 5G мрежите, и ii) други фактори, като например правната и политическата рамка, която може да важи за доставчиците на информационни и комуникационни технологии в трети държави.

4) Въз основа на тази национална оценка на риска и този преглед и вземайки предвид текущите координирани действия на равнището на Съюза, държавите членки следва:

а) да актуализират изискванията за сигурност и методите за управление на риска, прилагани по отношение на 5G мрежите;

б) да актуализират съответните задължения, наложени на предприятията, предоставящи обществени съобщителни мрежи или обществено достъпни електронни съобщителни услуги, в съответствие с членове 13а и 13б от Директива 2002/21/ЕО;

в) да добавят към общото разрешение условия относно защитата на обществените мрежи срещу неразрешен достъп и да поискат от предприятията, участващи в предстоящите процедури за предоставяне на права за ползване на радиочестоти в 5G лентите, да поемат ангажименти за спазване на изискванията за сигурност на мрежите в съответствие с Директива 2002/20/ЕО;

г) да прилагат други превантивни мерки за смекчаване на потенциалните рискове за киберсигурността.

5) Мерките, посочени в точка 4, следва да включват по-големи задължения за доставчиците и операторите с цел гарантиране на сигурността на чувствителните части от мрежите, както и, когато е уместно, задължения за предоставяне на компетентните национални органи на съответната информация за планирани промени в електронни съобщителни мрежи и изисквания за предварително подлагане на конкретните информационни компоненти и системи на изпитвания за сигурност и цялост от национални одитни/сертифициращи лаборатории.

6) Съвместните прегледи на сигурността следва да се извършват от две или повече държави членки, като се използват и споделят подходящите технически експертни знания и съоръжения, свързани с инфраструктурите в основата на цифровата екосистема и 5G мрежите, например когато едно и също предприятие извършва дейности или изгражда мрежова инфраструктура в повече от една държава членка или когато има значителни прилики между мрежовите конфигурации. Агенцията на Европейския съюз за киберсигурност (ENISA), Европол и Органът на европейските регулатори в областта на електронните съобщения (ОЕРЕС) следва да третират като приоритетни исканията на държавите членки за подкрепа в тази област. Резултатите от тези прегледи следва да бъдат предадени на групата за сътрудничество и мрежата на екипите за реагиране при инциденти с компютърната сигурност.

IV. **КООРДИНИРАНИ ДЕЙСТВИЯ НА РАВНИЩЕТО НА СЪЮЗА**

7) С цел разработване на общ подход за справяне с рисковете за киберсигурността по отношение на 5G мрежите държавите членки следва да започнат да работят специално в това направление в рамките на групата за сътрудничество до 30 април 2019 г. Държавите членки следва да поканят съответните органи да участват, когато това е уместно, в работата на групата за сътрудничество.

Координирана европейска оценка на риска

8) Държавите членки следва да обменят информация помежду си и със съответните органи на Съюза с цел постигане на обща осведоменост за съществуващите и потенциалните рискове за киберсигурността, свързани с 5G мрежите.

9) Държавите членки следва да предадат на Комисията и на Агенцията на Европейския съюз за киберсигурност (ENISA) своите национални оценки на риска до 15 юли 2019 г.

10) Агенцията на Европейския съюз за киберсигурност (ENISA) следва да извърши специален преглед на картината на заплахите за 5G мрежите. Групата за сътрудническо и мрежата на екипите за реагиране при инциденти с компютърната сигурност, създадени по силата на Директива (ЕС) 2016/1148, следва да подкрепят този процес.

11) До 1 октомври 2019 г., като вземат предвид всички тези елементи, държавите членки заедно с Агенцията на Европейския съюз за киберсигурност (ENISA) и с подкрепата на Комисията следва да извършат съвместен преглед на излагането в целия Съюз на рискове, свързани с инфраструктурите в основата на цифровата екосистема, и по-специално 5G мрежите.

12) В този съвместен преглед следва да се даде приоритет на анализа на рисковете, свързани с особено чувствителните или уязвими елементи, включени в основните елементи на 5G мрежите, с центъра за операции и поддръжка, както и с елементите на мрежата за 5G достъп, използвани за промишлени приложения.

13) През втората фаза този съвместен преглед следва да бъде разширен, за да включи другите стратегически елементи на цифровата верига на стойността.

Общ инструментариум на Съюза за справяне с рисковете

14) В своята работа групата за сътрудничество следва да идентифицира прилагани на национално равнище най-добри практики от вида, предвиден в точка 4. Въз основа на тези национални най-добри практики до 31 декември 2019 г. следва да бъде постигнато съгласие относно инструментариум от подходящи, ефективни и пропорционални мерки за управление на риска, с които се намаляват рисковете за киберсигурността, идентифицирани на национално равнище и равнището на Съюза, с цел консултиране на Комисията във връзка с разработването на минимални общи изисквания за гарантиране в още по-голяма степен на високо ниво на киберсигурност на 5G мрежите в целия Съюз.

15) Този инструментариум следва да включва:

а) опис на видовете рискове за сигурността, които могат да засегнат киберсигурността на 5G мрежите (напр. риск по веригата на доставки, риск, свързан със софтуерни уязвимости, риск, свързан с контрола на достъпа, рискове, произтичащи от правната и политическата рамка, която може да важи за доставчиците на информационни и комуникационни технологии в трети държави), както и

б) набор от възможни мерки за намаляване на риска (напр. сертифициране на хардуера, софтуера или услугите от трета страна, официални изпитвания на хардуера и софтуера или проверки за съответствие, процеси за гарантиране на наличието и прилагането на контрол на достъпа, идентифициране на продукти, услуги или доставчици, които се смятат за потенциално несигурни, и др.). Тези мерки следва да бъдат насочени към всички видове рискове за сигурността, които са идентифицирани в една или повече държави членки след оценката на риска.

16) След като се разработят европейски схеми за сертифициране на киберсигурността, които имат отношение към 5G мрежите, държавите членки следва да приемат в съответствие с правото на Съюза национални технически правила за задължително сертифициране на информационните и комуникационните продукти, услуги или системи, обхванати от тези схеми.

17) Държавите членки заедно с Комисията следва да определят условията относно защитата на обществените мрежи срещу неразрешен достъп, които да бъдат добавени към общото разрешение, и изисквания за сигурност на мрежите с цел отправяне на искания за поемане на ангажименти до предприятията, участващи в процедури за предоставяне на права за ползване на радиочестоти в 5G лентите в съответствие с Директива 2002/20/ЕО. Те трябва да бъдат отразени, когато това е възможно, в предприетите мерки по точка 4, буква в).

18) Държавите членки следва да си сътрудничат с Комисията за разработването на специфични изисквания за сигурност, които да могат да се прилагат в контекста на обществените поръчки, свързани с 5G мрежите. Това следва да включва задължителни изисквания за използване на схеми за сертифициране на киберсигурността при обществени поръчки, доколкото участието в тези схеми все още не е задължително за всички доставчици и оператори.

V. **ПРЕГЛЕД**

19) Държавите членки следва да си сътрудничат с Комисията за извършване на оценка на въздействието на настоящата препоръка до 1 октомври 2020 г. с оглед на определянето на подходящи бъдещи действия. При тази оценка следва да се вземат предвид резултатите от координираната оценка на риска на равнището на Съюза и инструментариума на Съюза.

Съставено в Страсбург на 26 март 2019 година.

За Комисията

Julian KING

Член на Комисията