



Брюксел, 21.4.2021 г.
COM(2021) 206 final

2021/0106 (COD)

Предложение за

РЕГЛАМЕНТ НА ЕВРОПЕЙСКИЯ ПАРЛАМЕНТ И НА СЪВЕТА

**ЗА ОПРЕДЕЛЯНЕ НА ХАРМОНИЗИРАНИ ПРАВИЛА ОТНОСНО
ИЗКУСТВЕНИЯ ИНТЕЛЕКТ (ЗАКОНОДАТЕЛЕН АКТ ЗА ИЗКУСТВЕНИЯ
ИНТЕЛЕКТ) И ЗА ИЗМЕНЕНИЕ НА НЯКОИ ЗАКОНОДАТЕЛНИ АКТОВЕ НА
СЪЮЗА**

{SEC(2021) 167 final} - {SWD(2021) 84 final} - {SWD(2021) 85 final}

ОБЯСНИТЕЛЕН МЕМОРАНДУМ

1. КОНТЕКСТ НА ПРЕДЛОЖЕНИЕТО

1.1. Основания и цели на предложението

Настоящият обяснителен меморандум придружава предложението за Регламент за определяне на хармонизирани правила относно изкуствения интелект (Законодателен акт за изкуствения интелект). Изкуственият интелект (ИИ) е бързо развиваща се съвкупност от технологии, които могат да донесат множество икономически и социални ползи по протежение на целия спектър от промишлени отрасли и социални дейности. Чрез подобро прогнозиране, оптимизиране на операциите, разпределение на ресурсите и персонализиране на предоставянето на услуги използването на изкуствен интелект може да подпомогне постигането на резултати, които са благоприятни за обществото и околната среда, и да осигури ключови конкурентни предимства за дружествата и европейската икономика. Подобни действия са особено необходими в секторите със социално или екологично въздействие, включително изменението на климата, околната среда и здравеопазването, публичния сектор, финансите, мобилността, вътрешните работи и селското стопанство. Елементите и техниките, от които произтичат социално-икономическите ползи от ИИ, могат обаче да доведат и до нови рискове или отрицателни последици за отделните лица или обществото. Предвид бързината на технологичните промени и възможните предизвикателства ЕС се ангажира да се стреми към балансиран подход. В интерес на Съюза е да се запази технологичното лидерство на ЕС и да се гарантира, че европейците могат да се възползват от нови технологии, разработени и функциониращи в съответствие с ценностите, основните права и принципите на Съюза.

Настоящото предложение е в изпълнение на политическия ангажимент на председателя на Европейската комисия Урсула фон дер Лайен, която обяви в политическите си насоки за периода 2019—2024 г. „Съюз с по-големи амбиции“¹, че Комисията ще предложи законодателство за координиран европейски подход към човешките и етичните аспекти на ИИ. В продължение на това съобщение на 19 февруари 2020 г. Комисията публикува бялата книга относно ИИ – „Европа в търсене на високи постижения и атмосфера на доверие“². В бялата книга се определят варианти на политиката за това как да се постигне двойната цел за насърчаване на внедряването на ИИ и за справяне с рисковете, свързани с някои приложения на тези технологии. Задачата на настоящото предложение е, като предложи правна рамка за надежден ИИ, да изпълни втората цел за създаване на екосистема на доверие. В основата на предложението са ценностите на ЕС и основните права, като целта му е да даде на отделния човек и на другите ползватели увереност да възприемат основани на ИИ решения и същевременно да насърчи предприемачите да разработват такива решения. ИИ следва да бъде инструмент на разположение на човека и движеща сила за благо на обществото, като крайната цел е да се постигне по-голямо човешко благополучие. Поради това правилата за ИИ, предлаган на пазара на Съюза или засягащ по друг начин лица в Съюза, следва да бъдат ориентирани към човека, така че хората да имат увереността, че технологията се използва по безопасен и съответстващ на закона начин, включително по отношение на зачитането на основните права. След публикуването на

¹ https://ec.europa.eu/commission/sites/beta-political/files/political-guidelines-next-commission_en.pdf

² Европейска комисия, Бяла книга за изкуствения интелект — Европа в търсене на високи постижения и атмосфера на доверие, COM(2020) 65 final, 2020.

бялата книга Комисията започна консултация на широка основа със заинтересованите страни. Тя беше посрещната с голям интерес от голям брой заинтересовани страни, които като цяло подкрепиха регулаторната намеса за справяне с предизвикателствата и опасенията, породени от нарастващото използване на ИИ.

Предложението е също така в отговор на изричните искания от страна на Европейския парламент (ЕП) и Европейския съвет, които многократно са призовавали за законодателни действия, с които да се гарантира един добре функциониращ вътрешен пазар за системите с изкуствен интелект („системи с ИИ“), в който и ползите, и рисковете, свързани с ИИ, са адекватно третирани на равнището на Съюза. То подкрепя целта на Съюза да бъде световен лидер в развитието на сигурен, надежден и етичен изкуствен интелект, както посочи Европейският съвет³, и гарантира защитата на етичните принципи, както специално беше поискано от Европейския парламент⁴.

През 2017 г. Европейският съвет призова „спешно да се отговори на очертаващите се тенденции“, включително на „въпроси като изкуствения интелект [...], като в същото време се гарантира високо ниво на защита на данните, цифровите права и етичните стандарти.“⁵ В заключенията си от 2019 г. относно координирания план за развитие и използване на изкуствен интелект, произведен в Европа⁶, Съветът подчерта също така, че е важно да се гарантира, че правата на европейските граждани се зачитат в пълна степен, и призова за преразглеждане на действащото законодателство в тази област, за да бъде то пригодно за новите възможности и предизвикателства, породени от ИИ. Европейският съвет призова също за ясно определяне на приложенията с ИИ, които следва да се считат за високорискови⁷.

В последните заключения от 21 октомври 2020 г. се призовава и за преодоляване на непрозрачността, сложността, предубедеността, известната степен на непредвидимост и частично автономното поведение на някои системи с ИИ, за да се гарантира тяхната съвместимост с основните права и да се улесни прилагането на правните норми⁸.

Европейският парламент също има значителна дейност в областта на ИИ. През октомври 2020 г. той прие редица резолюции, свързани с ИИ, включително относно етиката⁹, отговорността¹⁰ и авторското право¹¹. През 2021 г. те бяха последвани от

³ Европейски съвет, [извънредно заседание на Европейския съвет \(1—2 октомври 2020 г.\) – Заключение](#), EUCO 13/20, 2020 г., стр. 6.

⁴ Резолюция на Европейския парламент от 20 октомври 2020 г. с препоръки към Комисията относно рамка за етичните аспекти на изкуствения интелект, роботиката и свързаните с тях технологии, 2020/2012(INL).

⁵ Европейски съвет, [заседание на Европейския съвет \(19 октомври 2017 г.\) – Заключение](#), EUCO 14/17, 2017 г., стр. 8.

⁶ Съвет на Европейския съюз, [Изкуствен интелект — б\) Заключение относно координирания план за изкуствения интелект — Приемане](#) 6177/19, 2019 г.

⁷ Европейски съвет, [извънредно заседание на Европейския съвет \(1 и 2 октомври 2020 г.\) – Заключение](#), EUCO 13/2020 г.

⁸ Съвет на Европейския съюз, [Заключения на председателството – Хартата на основните права в контекста на изкуствения интелект и цифровата промяна](#), 11481/20, 2020 г.

⁹ Резолюция на Европейския парламент от 20 октомври 2020 г. относно рамка за етичните аспекти на изкуствения интелект, роботиката и свързаните с тях технологии [2020/2012\(INL\)](#).

¹⁰ Резолюция на Европейския парламент от 20 октомври 2020 г. относно режим на гражданска отговорност за изкуствения интелект, [2020/2014\(INL\)](#).

¹¹ Резолюция на Европейския парламент от 20 октомври 2020 г. относно правата върху интелектуалната собственост за разработването на технологии за изкуствен интелект, [2020/2015\(INI\)](#).

резолюции относно ИИ в сферата на наказателноправните въпроси¹² и в областта на образованието, културата и аудио-визията¹³. В резолюцията на ЕП относно рамка от етични аспекти на изкуствения интелект, роботиката и свързаните с тях технологии изрично се препоръчва на Комисията да предложи законодателни действия за оползотворяване на възможностите и ползите от ИИ, но и за гарантиране на защитата на етичните принципи. Резолюцията включва текст на законодателно предложение за регламент относно етичните принципи за разработването, внедряването и използването на ИИ, роботиката и свързаните с тях технологии. В съответствие с политическия ангажимент, поет от председателя на ЕК Урсула фон дер Лайен в нейните политически насоки по отношение на резолюциите, приети от Европейския парламент съгласно член 225 от ДФЕС, настоящото предложение взема предвид горепосочената резолюция на Европейския парламент при пълно зачитане на принципите на пропорционалност, субсидиарност и по-добро законотворчество.

В този политически контекст Комисията излиза с предложената регулаторна рамка за изкуствения интелект, като си поставя следните **конкретни цели**:

- да гарантира, че системите с ИИ, които се пускат на пазара на Съюза и се използват, са безопасни и в съответствие с действащото законодателство в областта на основните права и ценностите на Съюза;
- да гарантира правна сигурност, която да улесни инвестициите и иновациите в ИИ;
- да подобри управлението и ефективното прилагане на съществуващата правна уредба в областта на основните права и изискванията за безопасност, приложими към системите с ИИ;
- да улесни развитието на единен пазар за законни, безопасни и надеждни приложения с ИИ и да предотврати разпокъсаност на пазара.

За постигането на тези цели в настоящото предложение се представя балансиран и пропорционален хоризонтален регулаторен подход към ИИ, който е ограничен до минималните необходими изисквания за справяне с рисковете и проблемите, свързани с ИИ, без да се ограничава неоправдано или възпрепятства технологичното развитие или по друг начин да се увеличават несъразмерно разходите за пускане на пазара на решения с ИИ. Предложена е стабилна и гъвкава правна рамка. От една страна, тя е всеобхватна и съобразена с бъдещето, що се отнася до основните регулаторни решения в нея, включително почиващите на принципи изисквания, на които следва да отговарят системите с ИИ. От друга страна, се въвежда пропорционална регулаторна система, в центъра на която стои ясно определен, основан на риска регулаторен подход, който не създава ненужни ограничения за търговията, като правната намеса е съобразена с конкретните ситуации, при които е налице основателна причина за безпокойство или

¹² Европейски парламент, проект на Доклад

относно изкуствения интелект в наказателното право и използването му от полицията и съдебните органи по наказателноправни въпроси [2020/2016\(INI\)](#).

¹³ Европейски парламент, проект на Доклад

относно изкуствения интелект в образованието, културата и аудио-визуалния сектор, [2020/2017\(INI\)](#). Във връзка с това Комисията прие Плана за действие в областта на цифровото образование за периода 2021—2027 г. — „Приспособяване на образованието и обучението към цифровата ера“ (съобщение на Комисията COM(2020) 624 final), в който се предвижда [разработването на етични насоки относно използването на ИИ и данни в образованието](#).

когато такова безпокойство може да се очаква в близко бъдеще. В същото време правната рамка включва гъвкави механизми, които ѝ позволяват да бъде динамично адаптирана спрямо развитието на технологията и появата на нови ситуации, предизвикващи безпокойство.

В предложението се определят хармонизирани правила за разработването, пускането на пазара и използването на системи с ИИ в Съюза, като се следва пропорционален подход, основан на риска. Предлага се единно, съобразено с бъдещето определение на ИИ. Някои особено вредни практики в сферата на ИИ са забранени като противоречащи на ценностите на Съюза, а по отношение на някои видове използване на системи за дистанционна биометрична идентификация за целите на правоприлагането се предлагат специални ограничения и предпазни мерки. С предложението се установява солидна методология по отношение на риска, за да се определят „високорисковите“ системи с ИИ, които представляват значителен риск за здравето и безопасността или за основните права на хората. Подобни системи с ИИ ще трябва да отговарят на набор от хоризонтални задължителни изисквания за надежден ИИ и да преминат през процедури за оценяване на съответствието, преди да могат да бъдат пуснати на пазара на Съюза. По отношение на доставчиците и ползвателите на подобни системи се определят предвидими, пропорционални и ясни задължения за гарантиране на безопасността и спазването на съществуващото законодателство за защита на основните права през целия жизнен цикъл на системите с ИИ. За някои специфични системи с ИИ се предлагат само минимални задължения за прозрачност, по-специално при използването на чатботове или т.нар. „дълбинни фалшификати“.

Предложените правила ще бъдат прилагани чрез система за управление на равнището на държавите членки, която се основава на вече съществуващи структури, и механизъм за сътрудничество на равнището на Съюза, който ще бъде осигурен със създаването на Европейски съвет по изкуствен интелект. Предлагат се и допълнителни мерки в подкрепа на иновациите, по-специално чрез т.нар. регулаторни лаборатории в областта на ИИ и други мерки за намаляване на регулаторната тежест и за подкрепа на малките и средните предприятия (МСП) и стартиращите предприятия.

1.2. Съгласуваност с действащите разпоредби в тази област на политиката

Хоризонталният характер на предложението изисква пълна съгласуваност със съществуващото законодателство на Съюза, приложимо в секторите, в които вече се използват високорискови системи с ИИ или е вероятно такива да се използват в близко бъдеще.

Гарантира се също така съгласуваността с Хартата на основните права на ЕС и действащото вторично законодателство на Съюза в областта на защитата на данните, защитата на потребителите, недискриминацията и равенството между половете. Предложението не засяга Общия регламент относно защитата на данните (Регламент (ЕС) 2016/679) и Директивата относно правоприлагането (Директива (ЕС) 2016/680), а ги допълва с набор от хармонизирани правила, приложими за проектирането, разработването и използването на някои високорискови системи с ИИ, и с ограничения за някои видове използване на системи за дистанционна биометрична идентификация. Освен това предложението допълва съществуващото право на Съюза относно недискриминацията със специфични изисквания, чиято цел е да се сведе до минимум рискът от алгоритмична дискриминация, по-специално по отношение на проектирането и качеството на наборите от данни, използвани за разработването на системи с ИИ, както и със задължения за изпитване, управление на риска, документиране и надзор от

страна на човека през целия жизнен цикъл на системите с ИИ. Предложението не засяга прилагането на правото на Съюза в областта на конкуренцията.

Що се отнася до високорисковите системи с ИИ, които са защитни елементи на продукти, настоящото предложение ще бъде интегрирано в съществуващото секторно законодателство в областта на безопасността, за да се гарантира последователност, да се избегне дублирането и да се сведе до минимум допълнителната тежест. Що се отнася по-специално до високорисковите системи с ИИ, свързани с продукти, обхванати от законодателството от новата законодателна рамка (НЗР) (напр. машини, медицински изделия, детски играчки), изискванията за системите с ИИ, съдържащи се в настоящото предложение, ще бъдат проверявани като част от съществуващите процедури за оценяване на съответствието съгласно съответното законодателство от НЗР. Що се отнася до взаимодействието между изискванията, ако специфичните за системите с ИИ рискове за безопасността трябва да бъдат обхванати от изискванията по настоящото предложение, то законодателството от НЗР има за цел да гарантира цялостната безопасност на крайния продукт и поради това може да съдържа специфични изисквания по отношение на безопасното интегриране на система с ИИ в крайния продукт. Предложението за Регламент относно машините, което се приема в един и същи ден с настоящото предложение, напълно отразява този подход. По отношение на високорисковите системи с ИИ, свързани с продукти, обхванати от съответното законодателство от стария подход (напр. въздухоплаване, автомобили), настоящото предложение няма да има пряко приложение. Предварителните съществени изисквания за високорисковите системи с ИИ, определени в настоящото предложение, обаче ще трябва да бъдат взети предвид при приемането на съответното законодателство за изпълнение или делегирано законодателство по тези актове.

Що се отнася до системите с ИИ, предоставяни или използвани от регулирани кредитни институции, органите, отговарящи за надзора на законодателството на Съюза в областта на финансовите услуги, следва да бъдат определени за компетентни органи за надзор по изискванията в настоящото предложение, за да се гарантира съгласувано изпълнение на задълженията съгласно настоящото предложение и законодателството на Съюза в областта на финансовите услуги, когато системите с ИИ до известна степен са уредени имплицитно във връзка със системата за вътрешно управление на кредитните институции. За да се подобри още повече съгласуваността, процедурата за оценяване на съответствието и някои от процедурните задължения на доставчиците съгласно настоящото предложение са включени в процедурите по Директива 2013/36/ЕС относно достъпа до осъществяването на дейност от кредитните институции и относно пруденциалния надзор¹⁴.

Настоящото предложение е в съответствие и с приложимото законодателство на Съюза относно услугите, включително относно междинните услуги, регулирани от Директива 2000/31/ЕО за електронната търговия¹⁵, и неотдашното предложение на Комисията за Законодателен акт за цифровите услуги (ЗАЦУ)¹⁶.

¹⁴ Директива 2013/36/ЕС на Европейския парламент и на Съвета от 26 юни 2013 г. относно достъпа до осъществяването на дейност от кредитните институции и относно пруденциалния надзор върху кредитните институции и инвестиционните посредници, за изменение на Директива 2002/87/ЕО и за отмяна на директиви 2006/48/ЕО и 2006/49/ЕО (текст от значение за ЕИП) (ОВ L 176, 27.6.2013 г., стр. 338–436).

¹⁵ Директива 2000/31/ЕО на Европейския парламент и на Съвета от 8 юни 2000 г. относно някои правни аспекти на услугите на информационното общество, и по-специално на електронната

По отношение на системите с ИИ, които са компоненти на широкомащабни информационни системи в пространството на свобода, сигурност и правосъдие, управлявани от Агенцията на Европейския съюз за оперативното управление на широкомащабни информационни системи (eu-LISA), предложението няма да се прилага за системите с ИИ, пуснати на пазара или въведени в експлоатация преди изтичането на една година от датата на прилагане на настоящия регламент, освен ако замената или изменението на тези правни актове доведе до значителна промяна в проекта или предназначението на съответната система или системи с ИИ.

1.3. Съгласуваност с други политики на Съюза

Предложението е част от по-широк всеобхватен пакет от мерки за справяне с проблемите, породени от развитието и използването на ИИ, в съответствие с анализа на Бялата книга за ИИ. Поради това се гарантира съгласуваност и взаимно допълване с други текущи или планирани инициативи на Комисията, които също имат за цел да разрешат тези проблеми, включително преразглеждането на секторното законодателство в областта на продуктите (напр. Директивата относно машините и Директивата относно общата безопасност на продуктите) и инициативите, насочени към въпроси на отговорността, свързани с новите технологии, включително системите с ИИ. Тези инициативи ще се основават на настоящото предложение и ще го допълнят, за да се постигне правна яснота и да се насърчи развитието на екосистема на доверие в ИИ в Европа.

Предложението е съгласувано с общата цифрова стратегия на Комисията в нейния принос за насърчаване на технологиите, работещи в полза на хората — един от трите основни стълба на насоката и целите на политиката, обявени в съобщението на Комисията „Изграждане на цифровото бъдеще на Европа“¹⁷. С него се създава съгласувана, ефективна и пропорционална рамка, за да се гарантира, че ИИ се разработва по начин, който зачита правата на хората и печели доверието им, подготвя Европа за цифровата ера и превръща следващите десет години в **цифрово десетилетие**¹⁸.

Освен това насърчаването на стимулираните от ИИ иновации е тясно свързано със **Законодателния акт за управлението на данните**¹⁹, **Директивата за отворените данни**²⁰ и други инициативи в рамките на **стратегията на ЕС за данните**²¹, чрез които ще се създадат ползващи се с доверие механизми и услуги за повторното използване, споделянето и обединяването на данни, които са от съществено значение за

търговия на вътрешния пазар („Директива за електронната търговия“), ОВ L 178, 17.7.2000 г., стр. 1—16.

¹⁶ Предложение за Регламент на Европейския парламент и на Съвета за Единен пазар на цифровите услуги (Законодателен акт за цифровите услуги) и за изменение на Директива 2000/31/ЕО, COM/2020/825 final.

¹⁷ Съобщение на Комисията „Изграждане на цифровото бъдеще на Европа“, COM/2020/67 final.

¹⁸ [Цифров компас 2030: Европейският път към цифровото десетилетие.](#)

¹⁹ Предложение за Регламент относно европейска рамка за управление на данните (Акт за управление на данните)

[COM/2020/767 final.](#)

²⁰ Директива (ЕС) 2019/1024 на Европейския парламент и на Съвета от 20 юни 2019 г. относно отворените данни и повторното използване на информацията от обществения сектор, PE/28/2019/REV/1, ОВ L 172, 26.6.2019 г., стр. 56—83.

²¹ [Съобщение на Комисията относно европейска стратегия за данните COM/2020/66 final.](#)

разработването на използващи данни висококачествени модели на ИИ.

С предложението също така се затвърждава значително ролята на Съюза в създаването на световни норми и стандарти и в насърчаването на надежден ИИ, който е в съответствие с ценностите и интересите на Съюза. То предоставя на Съюза стабилна основа за по-нататъшно взаимодействие с неговите външни партньори, включително трети държави, както и на международни форуми по въпроси, свързани с ИИ.

2. ПРАВНО ОСНОВАНИЕ, СУБСИДИАРНОСТ И ПРОПОРЦИОНАЛНОСТ

2.1. Правно основание

Правното основание на предложението е на първо място член 114 от Договора за функционирането на Европейския съюз (ДФЕС), в който се предвижда въвеждането на мерки, които да гарантират изграждането и функционирането на вътрешния пазар.

Предложението представлява основна част от стратегията на ЕС за цифровия единен пазар. Основната цел на настоящото предложение е да се гарантира правилното функциониране на вътрешния пазар, като се определят хармонизирани правила, по-специално относно разработването, пускането на пазара на Съюза и използването на продукти и услуги, използващи технологии с ИИ или предоставяни като самостоятелни системи с ИИ. Някои държави членки вече обмислят възможността за приемане на национални правила, за да гарантират, че ИИ е безопасен и се разработва и използва в съответствие със задълженията, свързани с основните права. Това вероятно ще доведе до два основни проблема: i) раздробяване на вътрешния пазар по отношение на съществените елементи, по-специално по отношение на изискванията за продуктите и услугите с ИИ, тяхното предлагане на пазара, използването им, отговорността и надзора от страна на публичните органи и ii) значително намаляване на правната сигурност както за доставчиците, така и за ползвателите на системи с ИИ относно начина, по който съществуващите и новите правила ще се прилагат за тези системи в Съюза. Като се има предвид активното трансгранично движение на продукти и услуги, тези два проблема могат да бъдат решени най-добре чрез законодателство на ЕС за хармонизация.

В предложението съответно се определят общи задължителни изисквания, приложими към проектирането и разработката на определени системи с ИИ, преди те да бъдат пуснати на пазара, които ще бъдат приведени по-нататък в действие чрез хармонизирани технически стандарти. В предложението се разглежда и ситуацията след пускането на пазара на системи с ИИ, като се хармонизира начинът, по който се извършват последващите проверки.

Освен това, като се има предвид, че настоящото предложение съдържа някои специални правила за защита на физическите лица по отношение на обработването на лични данни, по-специално ограничения за използването на системи с ИИ за дистанционна биометрична идентификация в реално време на обществено достъпни места за целите на правоприлагането, е целесъобразно правното основание на настоящия регламент, що се отнася до тези специфични правила, да бъде член 16 от ДФЕС.

2.2. Субсидиарност (при неизключителна компетентност)

По своето естество ИИ често разчита на големи и разнообразни набори от данни и може да бъде вграден във всеки продукт или услуга, ползващи се от свободно движение в рамките на вътрешния пазар, и това предполага, че целите на настоящото предложение не могат да бъдат ефективно постигнати самостоятелно от държавите членки. Освен това една нововъзникваща разпокъсана рамка от потенциално разминаващи се национални правила ще възпрепятства безпроблемното движение в целия ЕС на продукти и услуги, свързани със системи с ИИ, и ще бъде неефективна като гаранция на безопасността и защитата на основните права и ценностите на Съюза в различните държави членки. Националните подходи за справяне с проблемите само ще създадат допълнителна правна несигурност и пречки и ще забавят навлизането на ИИ на пазара.

Целите на настоящото предложение могат да бъдат постигнати по-добре на равнището на Съюза, за да се избегне допълнително раздробяване на единния пазар на потенциално противоречащи си национални рамки, които възпрепятстват свободното движение на стоки и услуги, включващи ИИ. Една стабилна европейска регулаторна рамка за надежден ИИ ще осигури също така еднакви условия на конкуренция и ще защити всички хора, като същевременно ще укрепи конкурентоспособността и промишлената база на Европа в областта на ИИ. Само общи действия на равнището на Съюза могат също така да защитят цифровия суверенитет на Съюза и да задействат неговите инструменти и регулаторни правомощия за създаване на световни правила и стандарти.

2.3. Пропорционалност

Предложението се основава на съществуващите правни рамки и е пропорционално и необходимо за постигане на преследваните цели, тъй като следва основан на риска подход и налага регулаторна тежест само когато има вероятност дадена система с ИИ да представлява висок риск за основните права и безопасността. За останалите, невисокорискови системи с ИИ се налагат само много ограничени задължения за прозрачност, например по отношение на предоставянето на информация, от която да става ясно за взаимодействащите хора, че се използва система с ИИ. За високорисковите системи с ИИ изискванията за висококачествени данни, документация и проследимост, прозрачност, човешки надзор, точност и надеждност са абсолютно необходими за смекчаване на рисковете за основните права и безопасността, породени от ИИ и необхванати от други съществуващи правни рамки. Едни хармонизирани стандарти и подкрепящи насоки и инструменти за постигане на съответствие ще помогнат на доставчиците и потребителите да спазват изискванията, определени в предложението, и ще сведат до минимум техните разходи. Разходите за операторите са пропорционални на постиганите цели и на икономическите и репутационните ползи, които те могат да очакват от настоящото предложение.

2.4. Избор на инструмент

Изборът на регламент като правен инструмент е оправдан от необходимостта от еднакво прилагане на новите правила, като например определението за ИИ, забраната на някои вредни практики, които използването на ИИ прави възможни, и класификацията на някои системи с ИИ. Пряката приложимост на регламента в съответствие с член 288 от ДФЕС ще намали правната разпокъсаност и ще улесни изграждането на единен пазар за законни, безопасни и надеждни системи с ИИ. Това ще бъде постигнато по-специално чрез въвеждането на хармонизиран набор от основни изисквания по отношение на системите с ИИ, класифицирани като високорискови, и на

задължения за доставчиците и ползвателите на тези системи, с които се подобрява защитата на основните права и се гарантира правна сигурност както за операторите, така и за потребителите.

В същото време разпоредбите на регламента не са прекалено предписателни и оставят възможност за различни равнища на действие от страна на държавите членки по отношение на елементи, които не подкопават целите на инициативата, по-специално вътрешната организация на системата за надзор на пазара и въвеждането на мерки за насърчаване на иновациите.

3. РЕЗУЛТАТИ ОТ ПОСЛЕДВАЩИТЕ ОЦЕНКИ, КОНСУЛТАЦИИТЕ СЪС ЗАИНТЕРЕСОВАНИТЕ СТРАНИ И ОЦЕНКИТЕ НА ВЪЗДЕЙСТВИЕТО

3.1. Консултации със заинтересованите страни

Настоящото предложение е резултат от обширни консултации с всички основни заинтересовани страни, при които бяха приложени общите принципи и минималните стандарти за консултациите със заинтересовани страни от страна на Комисията.

Заедно с публикуването на Бялата книга за изкуствения интелект на 19 февруари 2020 г. започна **обществена онлайн консултация**, която продължи до 14 юни 2020 г. Целта на консултацията беше да се съберат мнения и становища относно бялата книга. Тя беше насочена към всички заинтересовани страни от публичния и частния сектор, включително държавно управление, местни органи, търговски и нетърговски организации, социални партньори, експерти, представители на академичните среди и граждани. След анализ на всички получени отговори Комисията публикува на уебсайта си резюме на резултатите и отделните отговори²².

Бяха получени общо 1215 отговора, от които 352 от дружества или бизнес организации/асоциации, 406 от физически лица (92 % физически лица от ЕС), 152 от името на академични/изследователски институции и 73 от публични органи. Мненията на гражданското общество бяха представени от 160 респонденти (от които 9 организации на потребители, 129 неправителствени организации и 22 профсъюза), 72 респонденти участваха като „други“. От 352 представители на бизнеса и промишлеността 222 са дружества и представители на бизнеса, 41,5 % от които са микро-, малки и средни предприятия. Останалите са бизнес асоциации. Като цяло 84 % от отговорите на бизнеса и промишлеността са от ЕС-27. За различните въпроси между 81 и 598 от респондентите са използвали възможността за добавяне на свободен текст, за да направят коментари. Чрез уебсайта на EU Survey бяха предоставени над 450 документа за изразяване на позиция — в допълнение към отговорите на въпросника (над 400) или подадени отделно (над 50).

Като цяло е налице съгласие между заинтересованите страни относно необходимостта от действия. Голяма част от заинтересованите страни са съгласни, че в законодателството има празноти или че е необходимо ново законодателство. Няколко заинтересовани страни обаче предупреждават Комисията да избягва дублиране, противоречащи си задължения и свръхрегулиране. В много коментари се подчертава значението на технологично неутралната и пропорционална регулаторна рамка.

Заинтересованите страни искат най-вече тясно, ясно и точно определение за ИИ. Заинтересованите страни подчертаха също така, че освен изясняването на понятието

²² [Вижте всички резултати от консултацията тук.](#)

„ИИ“ е важно да се даде определение на понятията „риск“, „високорисков“, „нискорисков“, „дистанционна биометрична идентификация“ и „вреда“.

Повечето респонденти изрично подкрепят подхода, основан на риска. Използването на рамка, основана на риска, се счита за по-добър вариант от общото регулиране на всички системи с ИИ. Видовете рискове и заплахи следва да се основават на отделен за всеки сектор и случай подход. Рисковете следва също така да се оценяват с оглед на отражението върху правата и безопасността.

Регулаторните лаборатории биха могли да бъдат много полезни за насърчаването на ИИ и се приветстват от някои заинтересовани страни, особено бизнес асоциациите.

Сред тези, които са изразили своето становище относно моделите на правоприлагане, повече от 50 %, особено от средите на бизнес асоциациите, са за комбинация от предварителна самостоятелна оценка на риска и последващо прилагане на разпоредбите за високорисковите системи с ИИ.

3.2. Събиране и използване на експертни становища

Предложението се основава на проведен в продължение на две години анализ и тясно участие на заинтересованите страни, включително академичните среди, предприятията, социалните партньори, неправителствените организации, държавите членки и гражданите. Подготвителната работа започна през 2018 г. със създаването на **експертна група на високо равнище по въпросите на изкуствения интелект (ЕГВР)**, в която бяха представени всички заинтересовани страни и чийто разнообразен състав включваше 52-ма добре известни експерти със задачата да съветват Комисията относно изпълнението на нейната стратегия за изкуствения интелект. През април 2019 г. Комисията подкрепи²³ ключовите изисквания, определени в Насоките на ЕГВР относно етичните аспекти за надежден ИИ²⁴, които бяха преразгледани така, че да се вземат предвид над 500 становища от заинтересовани страни. Основните изисквания отразяват широкоразпространен и общ подход, както е видно от множество етични кодекси и принципи, разработени от много частни и публични организации в Европа и извън нея. Според него разработването и използването на ИИ следва да се ръководи от някои основни принципи с ценностна ориентация. Списъкът за оценка на надеждността на изкуствения интелект (СОНИИ)²⁵ въведе тези изисквания в практиката в рамките на пилотен процес с над 350 организации.

Освен това **Алиансът за ИИ**²⁶ беше създаден като платформа за около 4000 заинтересовани страни за обсъждане на технологичните и обществените последици от ИИ, което завърши с годишна асамблея по въпросите на ИИ.

Бялата книга за ИИ доразви този приобщаващ подход и стана причина над 1250 заинтересовани страни да изпратят своите коментари наред с над 450 становища. В резултат на това Комисията публикува една първоначална оценка на въздействието, по

²³ Европейска комисия, [Изграждане на доверие в ориентирания към човека изкуствен интелект](#), COM(2019) 168.

²⁴ ЕГВР, [Насоки относно етичните аспекти за надежден ИИ](#), 2019 г.

²⁵ ЕГВР, [Списък за оценка на надеждността на изкуствения интелект \(СОНИИ\) за целите на самооценката](#), 2020 г.

²⁶ Алиансът за ИИ е форум с участието на множество заинтересовани страни, чието начало беше поставено през юни 2018 г., Алианс за ИИ <https://ec.europa.eu/digital-single-market/en/european-ai-alliance>

която също бяха получени над 130 коментара²⁷. Бяха организирани и допълнителни семинари и мероприятия със заинтересованите страни, резултатите от които подкрепят анализа в оценката на въздействието и избраните в настоящото предложение политически варианти²⁸. Беше поръчано и външно проучване, което да бъде включено в оценката на въздействието.

3.3. Оценка на въздействието

В съответствие със своята политика за „по-добро регулиране“ Комисията извърши оценка на въздействието на настоящото предложение, разгледана от Комитета за регулаторен контрол на Комисията. На 16 декември 2020 г. беше проведена среща с Комитета за регулаторен контрол, която беше последвана от отрицателно становище. След съществено преразглеждане на оценката на въздействието в отговор на коментарите и повторното ѝ представяне, на 21 март 2021 г. Комитетът за регулаторен контрол излезе с положително становище. Становищата на Комитета за регулаторен контрол, препоръките и обяснение на начина, по който те са били взети предвид, са представени в приложение 1 към оценката на въздействието.

Комисията разгледа различни варианти на политиката за постигане на общата цел на предложението, която е да се гарантира правилното функциониране на единния пазар чрез създаване на условия за разработването и използването в Съюза на надежден ИИ.

Бяха оценени четири варианта на политика с различна степен на регулаторна намеса:

- **Вариант 1:** законодателен инструмент на ЕС за създаване на схема за доброволно обозначаване;
- **Вариант 2:** секторен „ad hoc“ подход;
- **Вариант 3:** хоризонтален законодателен инструмент на ЕС, следващ пропорционален подход, основан на риска;
- **Вариант 3+:** хоризонтален законодателен инструмент на ЕС, следващ пропорционален подход, основан на риска + кодекси за поведение за невисокорискови системи с ИИ;
- **Вариант 4:** хоризонтален законодателен инструмент на ЕС за установяване на задължителни изисквания за всички системи с ИИ, независимо от риска, който те представляват.

Съгласно установената от Комисията методология всеки вариант на политика бе оценен по отношение на неговото икономическо и обществено въздействие, като специално внимание беше отделено на въздействието върху основните права. Предпочитаният вариант е вариант 3+, а именно регулаторна рамка само за високорисковите системи с ИИ, с възможност всички доставчици на невисокорискови системи с ИИ да следват кодекс за поведение. Изискванията ще се отнасят до данни, документация и проследимост, предоставяне на информация и прозрачност, човешки надзор, надеждност и точност и ще бъдат задължителни за високорисковите системи с

²⁷ Европейска комисия, [Първоначална оценка на въздействието за предложение за правен акт на Европейския парламент и на Съвета за определяне на изискванията за изкуствения интелект.](#)

²⁸ За подробности относно всички проведени консултации вж. приложение 2 към оценката на въздействието.

ИИ. Дружествата, въвели кодекси за поведение за други системи с ИИ, ще направят това доброволно.

Предпочитаният вариант бе счетен за подходящ да отговори по най-ефективния начин на целите на настоящото предложение. Като изисква ограничен, но ефективен набор от действия от разработчиците и ползвателите на ИИ, предпочитаният вариант ограничава рисковете от нарушаване на основните права и безопасността на хората и насърчава ефективния надзор и правоприлагане чрез насочване на изискванията само към системи, в които съществува висок риск от такива нарушения. В резултат на това въпросният вариант свежда до минимум разходите за привеждане в съответствие, като по този начин се избягва ненужно забавяне на навлизането на пазара поради по-високи цени и разходи за привеждане в съответствие. За да се преодолеят евентуалните неблагоприятни последици за МСП, този вариант включва няколко разпоредби, които да им помогнат да постигнат съответствие и да намалят разходите си, сред които са създаването на регулаторни лаборатории и задължението за отчитане на интересите на МСП при определянето на таксите, свързани с оценяването на съответствието.

Предпочитаният вариант ще повиши доверието на хората в ИИ, дружествата ще се сдобият с повече правна сигурност и държавите членки няма да имат причина да предприемат едностранни действия, които биха могли да фрагментират единния пазар. По-голямото търсене в резултат на по-високото доверие, по-големият брой налични оферти благодарение на правната сигурност и липсата на пречки пред трансграничното движение на системи с ИИ е вероятно да се отразят много положително на единния пазар на ИИ. Европейският съюз ще продължи да способства за бързото разрастване на своята основана на ИИ екосистема от иновативни услуги и продукти, включващи технологии с ИИ, или самостоятелни системи с ИИ, което ще доведе до увеличаване на цифровата автономност.

Предприятията или публичните органи, които разработват или използват приложения с ИИ, представляващи висок риск за безопасността или основните права на гражданите, ще трябва да спазват специфични изисквания и задължения. Спазването на тези изисквания би довело до разходи в размер на приблизително 6000—7000 EUR за доставка на нормална високорискова система с ИИ на стойност около 170 000 EUR до 2025 г. За ползвателите на ИИ ще има и годишни разходи за времето, изразходвано за осигуряване на човешки надзор, когато това е целесъобразно, в зависимост от случая на използване. Те се оценяват на около 5000 EUR до 8000 EUR годишно. Разходите за проверка могат да възлязат на допълнителни 3000—7500 EUR за доставчиците на високорискови ИИ. Предприятията или публичните органи, които разработват или използват приложения с ИИ, които не са класифицирани като високорискови, ще имат само минимални задължения за предоставяне на информация. Те обаче биха могли да изберат да се обединят и заедно да приемат кодекс за поведение, за да следват подходящи изисквания и да гарантират, че техните системи с ИИ са надеждни. В такъв случай разходите биха били най-много толкова високи, колкото за високорисковите системи с ИИ, но най-вероятно биха били по-ниски.

Въздействието на вариантите на политиката върху различните категории заинтересовани страни (икономически оператори/предприятия; органи за оценяване на съответствието, органи по стандартизация и други публични органи; физически лица/граждани; изследователи) са обяснени подробно в приложение 3 към оценката на въздействието в подкрепа на настоящото предложение.

3.4. Пригодност и опростяване на законодателството

С настоящото предложение се установява задължение, което ще се прилага за доставчиците и ползвателите на високорискови системи с ИИ. За доставчиците, които разработват и пускат такива системи на пазара на Съюза, то ще създаде правна сигурност и ще гарантира, че няма да възникнат пречки пред трансграничното предоставяне на свързани с ИИ услуги и продукти. За дружествата, използващи ИИ, то ще способства за повече доверие сред техните клиенти. За националните публични администрации то ще насърчи общественото доверие в използването на ИИ и ще укрепи механизмите за правоприлагане (чрез въвеждане на европейски механизъм за координация, осигуряване на подходящ капацитет и улесняване на одитите на системите с ИИ с нови изисквания за документиране, проследимост и прозрачност). Освен това в рамката ще бъдат предвидени конкретни мерки в подкрепа на иновациите, включително регулаторни лаборатории и специфични мерки в подкрепа на малките ползватели и доставчиците на високорискови системи с ИИ, за да се съобразят с новите правила.

Предложението също така има за цел по-специално да укрепи конкурентоспособността и промишлената база на Европа в областта на ИИ. Гарантира се пълна съгласуваност със съществуващото секторно законодателство на Съюза, приложимо за системите с ИИ (напр. относно продуктите и услугите), което ще внесе допълнителна яснота и ще опрости прилагането на новите правила.

3.5. Основни права

Използването на ИИ с неговите специфични характеристики (напр. непрозрачност, сложност, зависимост от данни, автономно поведение) може да накърни редица основни права, залегнали в Хартата на основните права на ЕС („Хартата“). Настоящото предложение има за цел да гарантира високо равнище на защита на тези основни права, както и да се занимае с различните източници на рискове чрез ясно определен подход, основан на риска. С набор от изисквания за надежден ИИ и пропорционални задължения за всички участници във веригата за създаване на стойност предложението ще подобри и насърчи защитата на правата, залегнали в Хартата: правото на човешко достойнство (член 1), зачитането на личния живот и защитата на личните данни (членове 7 и 8), недискриминацията (член 21) и равенството между жените и мъжете (член 23). То има за цел да предотврати сковаващия ефект върху правото на свобода на изразяване на мнение (член 11) и свободата на събранията (член 12), да гарантира правото на ефективни правни средства за защита и на справедлив съдебен процес, правото на защита и презумпцията за невинност (членове 47 и 48), както и общия принцип на добра администрация. Освен това, като се има предвид приложимостта му в определени области, предложението ще окаже положително въздействие върху правата на редица специални групи, като например правото на работниците на справедливи и равни условия на труд (член 31), високото равнище на защита на потребителите (член 28), правата на детето (член 24) и интеграцията на хората с увреждания (член 26). Правото на високо равнище на опазване на околната среда и подобряването на качеството на околната среда (член 37) също са от значение, включително по отношение на здравето и безопасността на хората. Задълженията за предварителни изпитвания, управление на риска и човешки надзор също така ще улеснят зачитането на други основни права чрез свеждане до минимум на риска от погрешни или предубедени решения, подпомагани от ИИ, в ключови области, като образованието и обучението, заетостта, важните услуги, правоприлагането и съдебната система. В случай че все още се нарушават основни права, ще бъде осигурена

ефективна защита на засегнатите лица чрез гарантиране на прозрачност и проследимост на системите с ИИ в съчетание със строги последващи проверки.

Настоящото предложение налага някои ограничения на свободата на стопанска инициатива (член 16) и свободата на изкуствата и науката (член 13), за да се гарантира спазването на императивни съображения от обществен интерес, като здравето, безопасността, защитата на потребителите и защитата на други основни права (съгласно принципа за отговорни иновации), когато се разработват и използват високорискови технологии с ИИ. Тези ограничения са съразмерни и сведени до необходимия минимум за предотвратяване и ограничаване на сериозните рискове за безопасността и вероятните нарушения на основните права.

Засилените задължения за прозрачност също така няма да засегнат непропорционално правото на защита на интелектуалната собственост (член 17, параграф 2), тъй като ще бъдат ограничени само до минималната информация, необходима на физическите лица, за да упражняват правото си на ефективни правни средства за защита, и до необходимата прозрачност по отношение на надзорните и правоприлагащите органи в съответствие с техните пълномощия. Всяко разкриване на информация ще се извършва съгласно съответното законодателство в тази област, включително Директива (ЕС) 2016/943 относно защитата на неразкрити ноу-хау и търговска информация (търговски тайни) срещу тяхното незаконно придобиване, използване и разкриване. Когато е необходимо публичните органи и нотифицираните органи да получат достъп до поверителна информация или до изходния код с цел проверка на спазването на съществени задължения, те биват обвързвани от задължения за поверителност.

4. ОТРАЖЕНИЕ ВЪРХУ БЮДЖЕТА

Държавите членки ще трябва да определят надзорни органи, които да отговарят за изпълнението на законодателните изисквания. Тяхната надзорна функция би могла да се основава на съществуващи договорености, например по отношение на органите за оценяване на съответствието или надзора на пазара, но ще изисква достатъчни технологични експертни знания и човешки и финансови ресурси. В зависимост от съществуващата структура във всяка държава членка това може да изиска между 1 и 25 еквивалента на пълно работно време за всяка държава членка.

Подробен преглед на свързаните разходи е представен във „финансовата обосновка“ към настоящото предложение.

5. ДРУГИ ЕЛЕМЕНТИ

5.1. Планове за изпълнение и механизми за мониторинг, оценка и докладване

Осигуряването на надежден механизъм за мониторинг и оценка е от решаващо значение, за да се гарантира, че предложението действително ще постигне поставените в него конкретни цели. Комисията ще отговаря за това да наблюдава въздействието на предложението. Тя ще създаде система за регистриране на самостоятелни високорискови приложения с ИИ в публична база данни в целия ЕС. Тази регистрация ще позволи също така на компетентните органи, ползвателите и другите заинтересовани лица да проверят дали високорисковата система с ИИ отговаря на изискванията, определени в предложението, и да упражняват засилен надзор върху системите с ИИ, които представляват висок риск за основните права. За да запазват тази база данни, доставчиците на ИИ ще бъдат задължени да предоставят съдържателна

информация за своите системи и за оценяването на съответствието, извършено спрямо тях.

Освен това доставчиците на ИИ ще бъдат задължени да информират националните компетентни органи за сериозни инциденти или неизправности, които представляват нарушение на задълженията, свързани с основните права, веднага щом узнаят за тях, както и за всяко изземване или изтегляне от пазара на системи с ИИ. След това националните компетентни органи разследват инцидентите или неизправностите, събират цялата необходима информация и редовно я предават на Комисията с подходящи метаданни. Комисията ще допълва тази информация за инцидентите с подробен анализ на цялостния пазар на ИИ.

Тя ще публикува доклад за оценка и преглед на предложената рамка за ИИ пет години след датата, на която тя започне да се прилага.

5.2. Подробно разяснение на конкретните разпоредби на предложението

5.2.1. ОБХВАТ И ОПРЕДЕЛЕНИЯ (ДЯЛ I)

Дял I определя предмета на регламента и приложното поле на новите правила, които обхващат пускането на пазара, въвеждането в експлоатация и използването на системи с ИИ. В него са посочени и определенията, използвани в целия инструмент. Определението за система с ИИ в правната рамка има за цел да бъде възможно най-неутрално по отношение на технологиите и да бъде съобразено с бъдещето предвид бързите технологични и пазарни развития, свързани с ИИ. За да се осигури необходимата правна сигурност, дял I се допълва от приложение I, в което се съдържа подробен списък на подходите и техниките за развитието на ИИ, които Комисията ще адаптира в съответствие с технологичните новости. Ключовите участници по веригата за създаване на стойност в областта на ИИ също са ясно определени, като например доставчиците и ползвателите на системи с ИИ, които обхващат както публични, така и частни оператори, за да се гарантират еднакви условия на конкуренция.

5.2.2. ЗАБРАНЕНИ ПРАКТИКИ В СФЕРАТА НА ИЗКУСТВЕНИЯ ИНТЕЛЕКТ (ДЯЛ II)

В дял II се установява списък на забранените ИИ. Регламентът следва основан на риска подход, като разграничава употребите на ИИ, които създават i) неприемлив риск, ii) висок риск и iii) нисък или минимален риск. Списъкът на забранените практики в дял II включва всички системи с ИИ, чието използване се счита за неприемливо поради това, че противоречи на ценностите на Съюза, например чрез нарушаване на основните права. Забраните обхващат практики, които имат значителен потенциал да манипулират хората чрез сублиминални техники отвъд рамките на съзнаването от човека, или да използват уязвимите места на конкретни уязвими групи, като деца или хора с увреждания, с цел съществено да изменят поведението им по начин, който би могъл да причини на тях или на друго лице психологическа или физическа вреда. Други манипулативни или злоупотребяващи практики спрямо зрели хора, за които могат да спомогнат системите с ИИ, биха могли да бъдат обхванати от съществуващото законодателство в областта на защитата на данните, защитата на потребителите и цифровите услуги, което гарантира, че физическите лица са надлежно информирани и имат свободен избор да не бъдат подлагани на профилиране или други практики, които биха могли да повлияят на реакциите им. Предложението също така забранява социалния рейтинг въз основа на ИИ за общи цели, извършвано от публични органи. И накрая, използването на системи за биометрична идентификация от разстояние в

реално време на публично достъпни места за целите на правоприлагането също е забранено, освен ако се прилагат някои ограничени изключения.

5.2.3. ВИСОКОРИСКОВИ СИСТЕМИ С ИИ (ДЯЛ III)

Дял III съдържа специфични правила за системите с ИИ, които създават висок риск за здравето и безопасността или за основните права на физическите лица. В съответствие с основан на риска подход тези високорискови системи с ИИ са разрешени на европейския пазар при спазване на определени задължителни изисквания и предварително оценяване на съответствието. Класифицирането на дадена система с ИИ като високорискова се основава на предназначението на системата с ИИ в съответствие със съществуващото законодателство в областта на безопасността на продуктите. Следователно класифицирането като високорискова зависи не само от функцията, изпълнявана от системата с ИИ, но и от конкретната цел и условия, за които се използва тази система.

В дял III, глава 1 се определят правилата за класификация и се обособяват две основни категории високорискови системи с ИИ:

- системи с ИИ, предназначени да бъдат използвани като защитен елемент на продукти, които подлежат на предварително оценяване на съответствието от трета страна;
- други самостоятелни системи с ИИ с последици предимно за основните права, които са изрично изброени в приложение III.

Този списък на високорискови системи с ИИ в приложение III съдържа ограничен брой системи с ИИ, чиито рискове вече са се проявили или има вероятност да се проявят в близко бъдеще. За да се гарантира, че регламентът може да бъде адаптиран към нововъзникващите употреби и приложения на ИИ, Комисията може да разшири списъка на високорисковите системи с ИИ, използвани в някои предварително определени области, чрез прилагане на набор от критерии и методология за оценка на риска.

В глава 2 се определят правните изисквания за високорисковите системи с ИИ във връзка с данните и управлението им, съхраняването на документацията и записите, прозрачността и предоставянето на информация на ползвателите, човешкия надзор, надеждността, точността и сигурността. Предлаганите минимални изисквания вече се използват от много добросъвестни оператори и са резултат от двегодишна подготвителна работа, вследствие Насоките на ЕГВР относно етичните аспекти²⁹, в която участваха над 350 организации³⁰. Те съответстват до голяма степен и на други международни препоръки и принципи, които гарантират, че предложената рамка за ИИ е съвместима с приетото от международните търговски партньори на ЕС. Точните технически решения за постигане на съответствие с тези изисквания могат да бъдат предоставени чрез стандарти или други технически спецификации или да бъдат разработени по друг начин в съответствие с общите инженерни или научни познания по преценка на доставчика на системата с ИИ. Тази гъвкавост е особено важна, тъй като позволява на доставчиците на системи с ИИ да избират начина, по който да изпълнят

²⁹ Експертна група на високо равнище по въпросите на изкуствения интелект, [Насоки относно етичните аспекти за надежден ИИ](#), 2019 г.

³⁰ Те бяха одобрени и от Комисията в нейното съобщение от 2019 г. относно ориентирания към човека подход към ИИ.

приложимите към тях изисквания, отчитайки съвременния технически и научен напредък в тази област.

Глава 3 предвижда ясен набор от хоризонтални задължения за доставчиците на високорискови системи с ИИ. На ползвателите и другите участници по веригата за създаване на стойност в областта на ИИ се възлагат пропорционални задължения (напр. вносители, дистрибутори, упълномощени представители).

В глава 4 се определя рамката за участие на нотифицираните органи като независими трети страни в процедурите за оценяване на съответствието, докато в глава 5 подробно са обяснени процедурите за оценяване на съответствието, които трябва да се следват за всеки вид високорискова система с ИИ. Подходът за оценяване на съответствието има за цел да сведе до минимум тежестта за икономическите оператори, както и за нотифицираните органи, чийто капацитет трябва постепенно да се увеличава с течение на времето. Системите с ИИ, предназначени да бъдат използвани като защитни елементи за продукти, регламентирани от разпоредбите на новата законодателна рамка (например машини, играчки, медицински изделия и т.н.), ще подлежат на същите предварителни и последващи механизми за съответствие и правоприлагане, приложими за продуктите, от които са част. Основната разлика е, че предварителните и последващите механизми ще гарантират спазването не само на изискванията, установени от секторното законодателство, но и на изискванията, установени с настоящия регламент.

По отношение на самостоятелните високорискови системи с ИИ, посочени в приложение III, ще бъде създадена нова система за съответствие и правоприлагане. Това следва законодателния модел на новата законодателна рамка, прилаган чрез проверки за вътрешен контрол от страна на доставчиците, с изключение на системите за дистанционна биометрична идентификация, които ще подлежат на оценяване на съответствието от трета страна. Едно цялостно предварително оценяване на съответствието чрез вътрешни проверки, съчетано със строго последващо правоприлагане, би могло да бъде ефективно и разумно решение за тези системи, като се има предвид ранната фаза на регулаторната намеса и фактът, че секторът на ИИ е много иновативен и едва сега се натрупва експертен опит в областта на одита. Оценяването чрез вътрешни проверки за самостоятелните високорискови системи с ИИ би изисквало пълно, ефективно и надлежно документирано предварително съответствие с всички изисквания на регламента, както и съответствие с надеждни системи за управление на качеството и риска и за мониторинг след пускането на пазара. След като доставчикът е извършил съответното оценяване на съответствието, той следва да регистрира тези самостоятелни високорискови системи с ИИ в база данни на ЕС, която ще бъде управлявана от Комисията, за да се повиши обществената прозрачност и надзор и да се засили последващият надзор от страна на компетентните органи. За сметка на това, от съображения за съгласуваност със съществуващото законодателство в областта на безопасността на продуктите, оценяването на съответствието на системите с ИИ, които са защитни елементи на продукти, ще следва система с процедури за оценяване на съответствието от трета страна, които вече са установени съгласно съответното секторно законодателство в областта на безопасността на продуктите. Ще бъде необходимо повторно предварително оценяване на съответствието в случай на съществени изменения на системите с ИИ (и по-специално промени, които надхвърлят предварително определеното от доставчика в техническата му документация и проверено в момента на предварителното оценяване на съответствието).

5.2.4. ЗАДЪЛЖЕНИЯ ЗА ПРОЗРАЧНОСТ ЗА НЯКОИ СИСТЕМИ С ИИ (ДЯЛ IV)

Дял IV се отнася до някои системи с ИИ, за да се вземат предвид специфичните рискове от манипулиране, които те пораждат. Задълженията за прозрачност ще се прилагат за системи, които i) взаимодействат с хора, ii) се използват за разпознаване на емоции или за определяне на връзка със (социални) категории въз основа на биометрични данни или iii) генерират или манипулират съдържание („дълбинни фалшификати“). Когато хората взаимодействат със система с ИИ или техните емоции или характеристики се разпознават чрез автоматизирани средства, те трябва да бъдат информирани за това обстоятелство. Ако дадена система с ИИ се използва за генериране или манипулиране на изображение, аудио или видео съдържание, което значително прилича на автентично съдържание, следва да има задължение за оповестяване, че съдържанието се генерира чрез автоматизирани средства, като може да бъдат направени изключения за законни цели (правоприлагане, свобода на изразяване). Това позволява на хората да направят информиран избор или да прекратят своето взаимодействие в дадена ситуация.

5.2.5. МЕРКИ В ПОДКРЕПА НА ИНОВАЦИИТЕ (ДЯЛ V)

Дял V допринася за постигането на целта за създаване на благоприятна за иновациите, ориентирана към бъдещето и устойчива на смущения правна рамка. За тази цел в него националните компетентни органи се насърчават да създадат регулаторни лаборатории и се определя основна рамка по отношение на управлението, надзора и отговорността. Регулаторните лаборатории в областта на ИИ създават контролирана среда за изпитване на иновативни технологии за ограничен период от време въз основа на план за изпитване, договорен с компетентните органи. Дял V съдържа също така мерки за намаляване на регулаторната тежест за МСП и стартиращите предприятия.

5.2.6. УПРАВЛЕНИЕ И ИЗПЪЛНЕНИЕ (ДЯЛОВЕ VI, VII И VIII)

В дял VI се определят системите за управление на равнището на Съюза и на национално равнище. На равнището на Съюза с предложението се създава Европейски съвет по изкуствен интелект („Съвета по ИИ“), съставен от представители на държавите членки и на Комисията. Съветът по ИИ ще улеснява гладкото, ефективно и хармонизирано прилагане на настоящия регламент, като допринася за ефективното сътрудничество между националните надзорни органи и Комисията и предоставя съвети и експертен опит на Комисията. Той също така ще събира и обменя най-добри практики между държавите членки.

На национално равнище държавите членки ще трябва да определят един или повече национални компетентни органи и, измежду тях, националния надзорен орган за целите на надзора върху прилагането и изпълнението на регламента. Европейският надзорен орган по защита на данните ще действа като компетентен орган за надзор на институциите, агенциите и органите на Съюза, когато те попадат в обхвата на настоящия регламент.

Дял VII има за цел да улесни работата по мониторинга на Комисията и националните органи чрез създаването на обща за целия ЕС база данни за самостоятелни високорискови системи с ИИ с отражение предимно върху основните права. Базата данни ще се управлява от Комисията и ще се захранва с данни от доставчиците на системи с ИИ, от които ще се изисква да регистрират своите системи, преди да ги пуснат на пазара или по друг начин да ги въведат в експлоатация.

В дял VIII се определят задълженията за мониторинг и докладване за доставчиците на системи с ИИ по отношение на мониторинга и докладването след пускането на пазара и

разследването на инциденти и неизправности, свързани с ИИ. Органите за надзор на пазара също така ще контролират пазара и ще разследват спазването на задълженията и изискванията за всички високорискови системи с ИИ, които вече са пуснати на пазара. Органите за надзор на пазара ще разполагат с всички правомощия съгласно Регламент (ЕС) 2019/1020 относно надзора на пазара. Последващото правоприлагане следва да гарантира, че след като системата с ИИ бъде пусната на пазара, публичните органи разполагат с правомощия и ресурси, за да се намесват, в случай че системите с ИИ порождават неочаквани рискове, които изискват спешна намеса. Те също така ще следят за това операторите да спазват своите задължения съгласно регламента. Предложението не предвижда автоматично създаване на допълнителни органи на равнището на държавите членки. Следователно държавите членки могат да посочат (и да използват експертния опит на) съществуващи секторни органи, на които ще бъдат възложени и правомощия за наблюдение и прилагане на разпоредбите на регламента.

Всичко това не засяга съществуващата система и разпределението на правомощията за последващо гарантиране на спазването на задълженията, свързани с основните права в държавите членки. Когато това е необходимо за изпълнението на правомощията им, съществуващите органи за надзор и правоприлагане ще имат също така правото да изискват и да получават достъп до всяка документация, водена съгласно настоящия регламент, и при необходимост да изискват от органите за надзор на пазара да проведат изпитване на дадена високорискова система с ИИ чрез технически средства.

5.2.7. КОДЕКСИ ЗА ПОВЕДЕНИЕ (ДЯЛ IX)

С дял IX се установява рамка за създаването на кодекси за поведение, които имат за цел да поощрят доставчиците на невисокорискови системи с ИИ да прилагат доброволно задължителните изисквания за високорисковите системи с ИИ (посочени в дял III). Доставчиците на невисокорискови системи с ИИ могат сами да създават и прилагат кодекси за поведение. Тези кодекси може също така да включват доброволни ангажименти, свързани например с екологичната устойчивост, достъпността за хора с увреждания, участието на заинтересованите страни в проектирането и разработването на системи с ИИ и културно-личностното разнообразие на екипите от разработчици.

5.2.8. ЗАКЛЮЧИТЕЛНИ РАЗПОРЕДБИ (ДЯЛОВЕ X, XI И XII)

В дял X се подчертава задължението на всички страни да спазват поверителността на информацията и данните и се определят правила за обмена на информация, получена по време на прилагането на регламента. В дял X се съдържат също така мерки за гарантиране на ефективното прилагане на регламента чрез ефективни, пропорционални и възпиращи санкции при нарушения на разпоредбите.

В дял XI се определят правилата за упражняване на делегираните и изпълнителните правомощия. С настоящото предложение Комисията се оправомощава да приема, когато е целесъобразно, актове за изпълнение, за да се гарантира еднаквото прилагане на регламента, или делегирани актове за актуализиране или допълване на списъците в приложения I—VII.

Дял XII съдържа задължение за Комисията да оценява редовно необходимостта от актуализиране на приложение III и да изготвя редовни доклади относно оценката и прегледа на регламента. В него също така се определят заключителни разпоредби, включително диференциран преходен период за началната дата на прилагане на регламента, за да се улесни безпроблемното прилагане от всички заинтересовани страни.

Предложение за

РЕГЛАМЕНТ НА ЕВРОПЕЙСКИЯ ПАРЛАМЕНТ И НА СЪВЕТА

ЗА ОПРЕДЕЛЯНЕ НА ХАРМОНИЗИРАНИ ПРАВИЛА ОТНОСНО ИЗКУСТВЕНИЯ ИНТЕЛЕКТ (ЗАКОНОДАТЕЛЕН АКТ ЗА ИЗКУСТВЕНИЯ ИНТЕЛЕКТ) И ЗА ИЗМЕНЕНИЕ НА НЯКОИ ЗАКОНОДАТЕЛНИ АКТОВЕ НА СЪЮЗА

ЕВРОПЕЙСКИЯТ ПАРЛАМЕНТ И СЪВЕТЪТ НА ЕВРОПЕЙСКИЯ СЪЮЗ,

като взеха предвид Договора за функционирането на Европейския съюз, и по-специално членове 16 и 114 от него,

като взеха предвид предложението на Европейската комисия,

след предаване на проекта на законодателния акт на националните парламенти,

като взеха предвид становището на Европейския икономически и социален комитет³¹,

като взеха предвид становището на Комитета на регионите³²,

в съответствие с обикновената законодателна процедура,

като имат предвид, че:

- (1) Целта на настоящия регламент е да се подобри функционирането на вътрешния пазар чрез установяване на единна правна рамка, по-специално за разработването, предлагането на пазара и използването на изкуствен интелект в съответствие с ценностите на Съюза. Настоящият регламент се ръководи от няколко императивни съображения от обществен интерес, като например високо равнище на защита на здравето, безопасността и основните права. С него се гарантира свободното трансгранично движение на стоки и услуги на базата на ИИ, като по този начин не се допуска държавите членки да налагат ограничения върху разработването, предлагането на пазара и използването на системи с ИИ, освен ако това е изрично разрешено от настоящия регламент.
- (2) Системите с изкуствен интелект (системи с ИИ) могат лесно да бъдат внедрени в множество сектори на икономиката и сфери на обществото, включително в трансграничен план, и да се ползват от свободно движение в целия Съюз. Някои държави членки вече са проучили възможността за приемане на национални правила, за да гарантират, че изкуственият интелект е безопасен и се разработва и използва в съответствие със задълженията, свързани с основните права. Различаващите се национални правила могат да доведат до фрагментиране на вътрешния пазар и да намалят правната сигурност за операторите, които разработват или използват системи с ИИ. Поради това следва да се гарантира еднакво и високо равнище на защита в целия Съюз, като същевременно следва да се предотвратят различията, възпрепятстващи свободното движение на

³¹ ОВ С [...], [...] г., стр. [...].

³² ОВ С [...], [...] г., стр. [...].

системи с ИИ и свързани с тях продукти и услуги в рамките на вътрешния пазар, като за целта се определят еднакви задължения за операторите и се гарантира еднаква защита на императивните съображения от обществен интерес и на правата на лицата на целия вътрешен пазар на основание член 114 от Договора за функционирането на Европейския съюз (ДФЕС). Доколкото настоящият регламент съдържа специални правила за защита на физическите лица по отношение на обработването на лични данни във връзка с ограниченията за използването на системи с ИИ за дистанционна биометрична идентификация в реално време на обществено достъпни места за целите на правоприлагането, е целесъобразно правното основание на настоящия регламент, що се отнася до тези специфични правила, да бъде член 16 от ДФЕС. С оглед на тези специфични правила и защитата съгласно член 16 от ДФЕС е целесъобразно да се проведе консултация с Европейския комитет по защита на данните.

- (3) Изкуственият интелект е бързо развиваща се съвкупност от технологии, които могат да допринесат за множество икономически и социални ползи по протежение на целия спектър от промишлени отрасли и социални дейности. Като подобрява прогнозирането, оптимизирането на операциите и разпределянето на ресурсите и персонализирането на цифровите решения, които са на разположение на физическите лица и организациите, използването на изкуствен интелект може да осигури ключови конкурентни предимства за дружествата и да съдейства за постигането на социално и екологично благоприятни резултати, например в областта на здравеопазването, селското стопанство, образованието и обучението, управлението на инфраструктурата, енергетиката, транспорта и логистиката, обществените услуги, сигурността, правосъдието, ресурсната и енергийната ефективност, както и при смекчаването на последиците от изменението на климата и адаптирането към него.
- (4) Същевременно, в зависимост от обстоятелствата по отношение на конкретното му приложение и използване, изкуственият интелект може да доведе до рискове и да накърни обществените интереси и правата, защитени от правото на Съюза. Тези вреди могат да бъдат имуществени или неимуществени.
- (5) Поради това е необходима правна рамка на Съюза, с която се определят хармонизирани правила относно изкуствения интелект, за да се насърчи разработването, използването и навлизането на изкуствения интелект на вътрешния пазар и която също така осигурява високо равнище на защита на въпросите от обществен интерес, като здравето и безопасността и защитата на основните права, признати и защитени от правото на Съюза. За постигането на тази цел следва да бъдат установени правила, уреждащи пускането на пазара и въвеждането в експлоатация на някои системи с ИИ, и по този начин да се гарантира безпрепятственото функциониране на вътрешния пазар и да се даде възможност на тези системи да се ползват от принципа на свободно движение на стоки и услуги. С определянето на тези правила настоящият регламент подкрепя целта на Съюза да бъде световен лидер в развитието на сигурен, надежден и етичен изкуствен интелект, както бе посочено от Европейския съвет³³, и

³³

Европейски съвет, извънредно заседание на Европейския съвет (1—2 октомври 2020 г.) – Заключение, EUCO 13/20, 2020 г., стр. 6.

гарантира защитата на етичните принципи, както изрично бе поискано от Европейския парламент³⁴.

- (6) Понятието за система с ИИ следва да бъде ясно определено, за да се гарантира правна сигурност, като същевременно се осигури гъвкавост, за да се обхване бъдещото технологично развитие. Определението следва да се основава на ключовите функционални характеристики на софтуера, по-специално на способността за определен набор от цели, дефинирани от човека, да се генерират крайни резултати, като съдържание, прогнози, препоръки или решения, които оказват влияние върху средата, с която системата си взаимодейства, било то във физическо или цифрово измерение. Системите с ИИ могат да бъдат проектирани да функционират с различна степен на автономност и да се използват самостоятелно или като компонент на продукт, независимо дали системата е физически интегрирана в продукта (вградена) или обслужва функционалността на продукта, без да бъде интегрирана в него (невградена). Определението за система с ИИ следва да бъде допълнено от списък със специфични техники и подходи, използвани за нейното разработване, който да се актуализира с оглед на пазарните и технологичните промени чрез приемането на делегирани актове от Комисията за изменението на този списък.
- (7) Понятието биометрични данни, използвано в настоящия регламент, е в съответствие с и следва да се тълкува съобразно с понятието за биометрични данни, определено в член 4, параграф 14 от Регламент (ЕС) 2016/679 на Европейския парламент и на Съвета³⁵, член 3, параграф 18 от Регламент (ЕС) 2018/1725 на Европейския парламент и на Съвета³⁶ и член 3, параграф 13 от Директива (ЕС) 2016/680 на Европейския парламент и на Съвета³⁷.
- (8) Понятието за система за дистанционна биометрична идентификация, използвано в настоящия регламент, следва да се определи функционално като система с ИИ с предназначение идентифициране на физически лица от разстояние чрез сравняване на биометричните данни на дадено лице с биометричните данни, съдържащи се в референтна база данни, като ползвателят на системата с ИИ не знае предварително дали лицето ще присъства и може да бъде идентифицирано. Като се имат предвид техните различни характеристики и начини на използване, както и различните рискове, с които те са свързани, следва да се направи

³⁴ Резолюция на Европейския парламент от 20 октомври 2020 г. с препоръки към Комисията относно рамка за етичните аспекти на изкуствения интелект, роботиката и свързаните с тях технологии, 2020/2012(INL).

³⁵ 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).

³⁶ Регламент (ЕС) 2018/1725 на Европейския парламент и на Съвета от 23 октомври 2018 г. относно защитата на физическите лица във връзка с обработването на лични данни от институциите, органите, службите и агенциите на Съюза и относно свободното движение на такива данни и за отмяна на Регламент (ЕО) № 45/2001 и Решение № 1247/2002/ЕО (ОВ L 295, 21.11.2018 г., стр. 39).

³⁷ Директива (ЕС) 2016/680 на Европейския парламент и на Съвета от 27 април 2016 г. 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, и за отмяна на Рамково решение 2008/977/ПВР на Съвета (Директива относно правоприлагането в областта на защитата на данните) (ОВ L 119, 4.5.2016 г., стр. 89).

разграничение между системите, работещи в реално време, и системите за експост дистанционна биометрична идентификация. При системите, работещи в реално време, снемането на биометрични данни, сравнението и идентификацията се осъществяват мигновено, почти мигновено или при всички случаи без значително забавяне. В това отношение не следва да има възможност за заобикаляне на правилата на настоящия регламент относно използването в реално време на въпросните системи с ИИ и за целта в него следва да се уредят незначителните забавяния. Системите, работещи в реално време, предполагат използването на материал „на живо“ или „почти на живо“, като видеозапис от камера или друго устройство с подобна функция. За разлика от тях при експост системите биометричните данни вече са снети и сравняването и идентифицирането се извършват едва след значително забавяне. Това предполага материал, като снимки или видеозаписи от камери от вътрешна система за видеонаблюдение или от частни устройства, които са направени преди използването на системата по отношение на въпросните физически лица.

- (9) За целите на настоящия регламент понятието за обществено достъпно място следва да се разбира като означаващо всяко физическо място, което е достъпно за обществеността, независимо дали то е частна или публична собственост. Поради това понятието не включва места, които са частни по естеството си и обичайно не са свободно достъпни за трети страни, включително за правоприлагащи органи, освен ако тези страни са получили специална покана или разрешение, какъвто е случаят например с жилища, частни клубове, складове, фабрики. Онлайн пространства също не се включват, тъй като те не са физически места. Фактът обаче, че евентуално има определени условия за достъп до определено място, например входни билети или възрастови ограничения, не означава, че това място не е обществено достъпно по смисъла на настоящия регламент. Следователно в допълнение към обществените места като улици, съответните части на държавни сгради и по-голямата част от транспортната инфраструктура, местата като кина, театри, магазини и търговски центрове в обичайния случай също са обществено достъпни. Дали дадено място е достъпно за обществеността обаче следва да се определя отделно във всеки един случай, като се отчита спецификата на въпросната ситуация.
- (10) За да се гарантират еднакви условия на конкуренция и ефективна защита на правата и свободите на физическите лица в целия Съюз, правилата, установени с настоящия регламент, следва да се прилагат недискриминационно по отношение на доставчиците на системи с ИИ, независимо дали са установени в Съюза или в трета държава, както и за ползвателите на системи с ИИ, установени в Съюза.
- (11) Поради своето цифрово естество някои системи с ИИ следва да попадат в обхвата на настоящия регламент дори когато не се пускат на пазара, не се въвеждат в експлоатация и не се използват в Съюза. Такъв е например случаят с оператор, установен в Съюза, който сключва договор за определени услуги с оператор, установен извън Съюза, във връзка с дейност, която ще се извършва от система с ИИ, която би била определена като високорискова и резултатите от която засягат физически лица, намиращи се в Съюза. При тези обстоятелства системата с ИИ, използвана от оператора извън Съюза, би могла да обработва данни, които са законно събрани в Съюза и прехвърлени оттам, и да предоставя на сключилия договор оператор в Съюза резултата, получен на базата на тази обработка, без въпросната система с ИИ да е била пускана на пазара, въвеждана в експлоатация или използвана в Съюза. За да не се допусне заобикаляне на

настоящия регламент и да се гарантира ефективна защита на физическите лица, намиращи се в Съюза, настоящият регламент следва също така да се прилага за доставчиците и ползвателите на системи с ИИ, установени в трета държава, доколкото резултатът, получен от тези системи, се използва в Съюза. Независимо от това, за да се вземат предвид съществуващите договорености и специалните потребности от сътрудничество с чуждестранни партньори, с които се обменят информация и доказателства, настоящият регламент не следва да се прилага за публичните органи на трета държава и за международните организации, когато те действат в рамките на международни споразумения, сключени на национално или европейско равнище за сътрудничество в областта на правоприлагането и за съдебно сътрудничество със Съюза или с неговите държави членки. Такива споразумения са сключени двустранно между държави членки и трети държави или между Европейския съюз, Европол и други агенции на ЕС и трети държави и международни организации.

- (12) Настоящият регламент следва да се прилага и за институциите, службите, органите и агенциите на Съюза, когато те действат като доставчик или ползвател на система с ИИ. Системите с ИИ, разработени или използвани изключително за военни цели, следва да бъдат изключени от обхвата на настоящия регламент, когато това използване попада в изключителната сфера на общата външна политика и политика на сигурност, уредена в дял V от Договора за Европейския съюз (ДЕС). Настоящият регламент следва да не засяга прилагането на разпоредбите относно отговорността на междинните доставчици на услуги, определени в Директива 2000/31/ЕО на Европейския парламент и на Съвета [изменена от Законодателния акт за цифровите услуги].
- (13) За да се гарантира последователно и високо равнище на защита на обществените интереси по отношение на здравето, безопасността и основните права, следва да бъдат определени общи нормативни стандарти за всички високорискови системи с ИИ. Тези стандарти следва да бъдат в съответствие с Хартата на основните права на Европейския съюз (Хартата), да бъдат недискриминационни и да са в съответствие с международните търговски ангажименти на Съюза.
- (14) За да се въведе пропорционален и ефективен набор от задължителни правила за системите с ИИ, следва да се прилага ясно определен подход, основан на риска. В рамките на този подход видът и съдържанието на правилата следва да се адаптират към интензитета и периметъра на рисковете, които системите с ИИ могат да породят. Поради това е необходимо да се забранят някои практики в областта на изкуствения интелект, да се определят изисквания за високорисковите системи с ИИ и задължения за съответните оператори, както и да се определят задължения за прозрачност за някои системи с ИИ.
- (15) Макар изкуственият интелект да има многобройни полезни приложения, с тази технология може да се злоупотребява и тя може да предоставя нови и мощни инструменти за манипулативни и експлоататорски практики и практики за социален контрол. Тези практики са особено вредни и следва да бъдат забранени, тъй като противоречат на ценностите на Съюза за зачитане на човешкото достойнство, свободата, равенството, демокрацията и принципите на правовата държава и на основните права на Съюза, включително правото на недискриминация, защита на данните и неприкосновеността на личния живот, както и правата на детето.

- (16) Пускането на пазара, въвеждането в експлоатация и използването на някои системи с ИИ, предназначени да изменят човешкото поведение, при което са вероятни физически или психологически вреди, следва да бъдат забранени. Такива системи с ИИ използват сублиминални компоненти, които хората не могат да възприемат съзнателно, или използват уязвимостта на деца или пълнолетни лица, дължаща се на тяхната възраст или физически или психически увреждания. При това целта е значително да бъде изменено поведението на дадено лице по начин, който причинява или е вероятно да причини вреда на него самото или на друго лице. Наличието на такава цел не може да се предпоставя, ако изменянето на човешкото поведение се дължи на външни за системата с ИИ фактори, които са извън контрола на доставчика или ползвателя. Преследващата легитимни цели научноизследователска работа по отношение на тези системи с ИИ не следва да бъде възпрепятствана от забраната, ако тя не е равностойна на използване на системата с ИИ в отношения човек—машина, които излагат физически лица на вреда, и се провежда в съответствие с признатите етични стандарти за научни изследвания.
- (17) Системите с ИИ, генериращи социален рейтинг с общо предназначение по отношение на физически лица за използване от публични органи или от тяхно име, могат да доведат до дискриминационни резултати и изключването на определени групи. Те могат да нарушат правото на достойнство и недискриминация и ценностите на равенството и справедливостта. Подобни системи с ИИ оценяват или класифицират надеждността на физически лица въз основа на тяхното социално поведение в разнообразен контекст или на предполагаеми лични или личностни характеристики. Социалният ранкинг, получен от такива системи с ИИ, може да доведе до накърняващо или неблагоприятно третиране на физически лица или на цели групи от такива лица в социални контексти, които нямат връзка с контекста, в който първоначално са били генерирани или събрани данните, или до накърняващо третиране, което е непропорционално или неоправдано с оглед на тежестта, която се отдава на тяхното социално поведение; Поради това такива системи с ИИ следва да бъдат забранени.
- (18) Използването на системи с ИИ за дистанционна биометрична идентификация в реално време на физически лица на обществено достъпни места за целите на правоприлагането се счита за особено силно накърняващо правата и свободите на засегнатите лица, доколкото то може да засегне личния живот на голяма част от населението, да породи усещане за постоянно наблюдение и косвено да действа разубеждаващо по отношение на упражняването на свободата на събранията и други основни права. Освен това непосредственият ефект и ограничените възможности за допълнителни проверки или корекции във връзка с използването на такива системи, функциониращи в реално време, крият повишен риск за правата и свободите на лицата, засегнати от дейностите по правоприлагане.
- (19) Поради това използването на тези системи за целите на правоприлагането следва да бъде забранено, освен в три изчерпателно изброени и подробно определени ситуации, при които използването е строго необходимо за постигане на значителен обществен интерес, чиято важност надделява над поеманите рискове. Тези ситуации включват издирването на конкретни потенциални жертви на престъпления, включително изчезнали деца; някои заплахи за живота или физическата безопасност на физически лица или за терористично нападение;

както и откриването, локализирането, идентифицирането или преследването на извършители или заподозрени в извършването на престъпленията, посочени в Рамково решение 2002/584/ПВР на Съвета³⁸, ако те са наказуеми в съответната държава членка с лишаване от свобода или мярка за задържане с максимален срок не по-малко от 3 години, както е определено в законодателството на съответната държава членка. Прагът относно срока на лишаването от свобода или на мярката за задържане в съответствие с националното право спомага да се гарантира, че престъплението е достатъчно тежко, за да обоснове евентуално използването на системи за дистанционна биометрична идентификация в реално време. Освен това от 32-те престъпления, изброени в Рамково решение 2002/584/ПВР на Съвета, някои е по-вероятно да са практически по-релевантни от други, поради което за използването на биометрична дистанционна идентификация в реално време може да се предположи, че ще бъде необходимо и пропорционално в много различна степен за практическото откриване, локализиране, идентифициране или преследване на извършителя или заподозрения за различните изброени престъпления, особено като се имат предвид вероятните разлики в тяхната тежест, вероятност и мащаб на вредата или възможните отрицателни последици.

- (20) За да се гарантира, че тези системи се използват по отговорен и пропорционален начин, е важно също така да се определи, че във всяка от тези три изчерпателно изброени и подробно определени ситуации следва да се вземат предвид определени елементи, по-специално по отношение на естеството на ситуацията, във връзка с която е искането, и последиците от използването за правата и свободите на всички засегнати лица, както и гаранциите и условията, при които ще премине използването. Освен това използването на системи за дистанционна биометрична идентификация в реално време на обществено достъпни места за целите на правоприлагането следва да бъде обект на подходящи времеви и пространствени ограничения, като се вземат предвид по-специално доказателствата или индикациите относно заплахите, жертвите или извършителя. Референтната база данни на лицата следва да бъде подходяща за всеки случай на използване във всяка от трите посочени по-горе ситуации.
- (21) Всяко използване на система за дистанционна биометрична идентификация в реално време на обществено достъпни места за целите на правоприлагането следва да бъде обект на изрично и конкретно разрешение от съдебен орган или от независим административен орган на държава членка. Такова разрешение следва по принцип да се получи преди използването, освен в надлежно обосновани спешни случаи, т.е. ситуации, при които необходимостта от използване на въпросните системи е такава, че е практически и обективно невъзможно разрешение да бъде получено преди началото на използването. При такива спешни ситуации използването следва да бъде ограничено до абсолютно необходимия минимум и да бъде обект на подходящи гаранции и условия, както е определено в националното право и дефинирано в контекста на всеки отделен случай на спешно използване от самия правоприлагащ орган. Освен това в такива случаи правоприлагащият орган следва да се опита да получи разрешение възможно най-скоро, като посочи причините, поради които не е могъл да го поиска по-рано.

³⁸

Рамково решение 2002/584/ПВР на Съвета от 13 юни 2002 г. относно европейската заповед за арест и процедурите за предаване между държавите членки (ОВ L 190, 18.7.2002 г., стр. 1).

- (22) Също така е целесъобразно да се предвиди, в рамките на изчерпателната уредба, създадена с настоящия регламент, че такова използване на територията на държава членка в съответствие с настоящия регламент следва да бъде възможно само и доколкото въпросната държава членка е решила изрично да предвиди възможността за разрешаване на такова използване в подробните правила на националното си право. Следователно съгласно настоящия регламент държавите членки са свободни изобщо да не предвиждат такава възможност или да предвидят такава възможност само по отношение на някои от целите, посочени в настоящия регламент, които могат да оправдаят разрешеното използване.
- (23) Използването на системи с ИИ за дистанционна биометрична идентификация в реално време на физически лица на обществено достъпни места за целите на правоприлагането задължително включва обработването на биометрични данни. Правилата на настоящия регламент, които забраняват — с някои изключения — подобно използване и чието правно основание е член 16 от ДФЕС, следва да се прилагат като *lex specialis* по отношение на правилата относно обработването на биометрични данни, съдържащи се в член 10 от Директива (ЕС) 2016/680, като по този начин се регламентира изчерпателно това използване и свързаното с него обработване на биометрични данни. Поради това такова използване и обработване следва да бъде възможно само доколкото е съвместимо с рамката, установена с настоящия регламент, без да има възможност извън тази рамка компетентните органи, когато действат за целите на правоприлагането, да използват такива системи и да обработват такива данни във връзка с него на основанията, изброени в член 10 от Директива (ЕС) 2016/680. В този контекст настоящият регламент няма за цел да осигури правно основание на обработването на лични данни съгласно член 8 от Директива 2016/680. Използването обаче на системи за дистанционна биометрична идентификация в реално време на обществено достъпни места за цели, различни от целите на правоприлагането, включително от компетентни органи, не следва да бъде обхванато от специалната рамка относно такова използване за целите на правоприлагането, установена с настоящия регламент. Поради това използването за цели, различни от целите на правоприлагането, не следва да бъде предмет на изискването за разрешение съгласно настоящия регламент и приложимите подробни правила на националното право, които могат да го предвиждат.
- (24) Всяко обработване на биометрични данни и други лични данни, необходимо за използването на системи с ИИ за биометрична идентификация, различно от такова във връзка с използването на системи за дистанционна биометрична идентификация в реално време на обществено достъпни места за целите на правоприлагането, уредено в настоящия регламент, включително когато такива системи се използват от компетентните органи на обществено достъпни места за цели, различни от правоприлагане, следва да продължи да отговаря на всички изисквания, произтичащи, според случая, от член 9, параграф 1 от Регламент (ЕС) 2016/679, член 10, параграф 1 от Регламент (ЕС) 2018/1725 и член 10 от Директива (ЕС) 2016/680.
- (25) В съответствие с член 6а от Протокол № 21 относно позицията на Обединеното кралство и Ирландия по отношение на пространството на свобода, сигурност и правосъдие, приложен към ДЕС и към ДФЕС, Ирландия не е обвързана от заложените в член 5, параграф 1, буква г) и член 5, параграфи 2 и 3 от настоящия регламент правила, приети на основание член 16 от ДФЕС и отнасящи се до

обработването на лични данни от държавите членки при осъществяване на дейности, попадащи в обхвата на трета част, дял V, глава 4 или глава 5 от ДФЕС, когато Ирландия не е обвързана от правилата, уреждащи формите на съдебно сътрудничество по наказателноправни въпроси или на полицейско сътрудничество, в рамките на които трябва да бъдат съблюдавани разпоредбите, установени на основание член 16 от ДФЕС.

- (26) В съответствие с членове 2 и 2а от Протокол № 22 относно позицията на Дания, приложен към ДЕС и ДФЕС, Дания не е обвързана от, нито е обект на прилагане на заложените в член 5, параграф 1, буква г) и член 5, параграфи 2 и 3 от настоящия регламент правила, приети на основание член 16 от ДФЕС, отнасящи се до обработването на лични данни от държавите членки при осъществяването на дейности, попадащи в обхвата на трета част, дял V, глава 4 или глава 5 от ДФЕС.
- (27) Високорисковите системи с ИИ следва да се пускат на пазара на Съюза или да се въвеждат в експлоатация само ако отговарят на определени задължителни изисквания. Тези изисквания следва да гарантират, че високорисковите системи с ИИ, които се предлагат в Съюза или резултатите от които се използват по друг начин в Съюза, не представляват неприемливи рискове за важни обществени интереси на Съюза, признати и защитени от неговото право. Системите с ИИ, определени като високорискови, следва да бъдат ограничени до тези, които имат значително вредно въздействие върху здравето, безопасността и основните права на хората в Съюза, като при това се свежда до минимум всяко потенциално ограничаване на международната търговия, ако има такава.
- (28) Системите с ИИ биха могли да доведат до неблагоприятни последици за здравето и безопасността на хората, по-специално когато тези системи функционират като компоненти на продукти. В съответствие с целите на законодателството на Съюза за хармонизация — да се улесни свободното движение на продукти на вътрешния пазар и да се гарантира, че на пазара има само безопасни и съответстващи на изискванията продукти — е важно рисковете за безопасността, които могат да възникнат от даден продукт като цяло поради неговите цифрови компоненти, включително системи с ИИ, да бъдат надлежно предотвратени и смекчени. Например все по-автономните роботи, независимо дали в контекста на производството или на индивидуалната помощ и грижи, следва да могат да работят и да изпълняват функциите си безопасно в сложна среда. Аналогично, в сектора на здравеопазването, където рисковете за живота и здравето са особено високи, все по-усъвършенствените системи за диагностика и системите за подпомагане на човешките решения следва да бъдат надеждни и точни. Степента на неблагоприятно въздействие на системата с ИИ върху основните права, защитени от Хартата, е от особено значение, когато дадена система с ИИ се класифицира като високорискова. Тези права включват правото на човешко достойнство, правото на зачитане на личния и семейния живот, защитата на личните данни, свободата на изразяване на мнение и свободата на информация, свободата на събранията и сдруженията, както и недискриминацията, защитата на потребителите, правата на работниците, правата на хората с увреждания, правото на ефективни правни средства за защита и на справедлив съдебен процес, правото на защита и презумпцията за невинност, както и правото на добра администрация. В допълнение към тези права е важно да се подчертае, че децата имат специфични права, които са залегнали в член 24 от Хартата на ЕС и в Конвенцията на ООН за правата на

детето (допълнително разработени в Общ коментар № 25 по Конвенцията на ООН за правата на детето по отношение на цифровата среда), като и в двата акта се изисква да се отчита уязвимостта на децата и да се осигуряват защитата и грижите, необходими за тяхното добруване. Основното право на високо равнище на защита на околната среда, залегнало в Хартата и реализирано в политиките на Съюза, също следва да се взема предвид при оценката на сериозността на вредата, която дадена система с ИИ може да причини, включително във връзка с човешкото здраве и безопасност.

- (29) По отношение на високорисковите системи с ИИ, които са защитни компоненти на продукти или системи или които сами по себе си са продукти или системи, попадащи в обхвата на Регламент (ЕО) № 300/2008 на Европейския парламент и на Съвета³⁹, Регламент (ЕС) № 167/2013 на Европейския парламент и на Съвета⁴⁰, Регламент (ЕС) № 168/2013 на Европейския парламент и на Съвета⁴¹, Директива 2014/90/ЕС на Европейския парламент и на Съвета⁴², Директива (ЕС) 2016/797 на Европейския парламент и на Съвета⁴³, Регламент (ЕС) 2018/858 на Европейския парламент и на Съвета⁴⁴, Регламент (ЕС) 2018/1139 на Европейския парламент и на Съвета⁴⁵ и Регламент (ЕС) 2019/2144 на Европейския парламент и на Съвета⁴⁶, е целесъобразно тези актове да бъдат

³⁹ Регламент (ЕО) № 300/2008 на Европейския парламент и на Съвета от 11 март 2008 г. относно общите правила в областта на сигурността на гражданското въздухоплаване и за отмяна на Регламент (ЕО) № 2320/2002 (ОВ L 97, 9.4.2008 г., стр. 72).

⁴⁰ Регламент (ЕС) № 167/2013 на Европейския парламент и на Съвета от 5 февруари 2013 г. относно одобряването и надзора на пазара на земеделски и горски превозни средства (ОВ L 60, 2.3.2013 г., стр. 1).

⁴¹ Регламент (ЕС) № 168/2013 на Европейския парламент и на Съвета от 15 януари 2013 г. относно одобряването и надзора на пазара на дву- и триколесни превозни средства и четириколки (ОВ L 60, 2.3.2013 г., стр. 52).

⁴² Директива 2014/90/ЕС на Европейския парламент и на Съвета от 23 юли 2014 г. относно морското оборудване и за отмяна на Директива 96/98/ЕО на Съвета (ОВ L 257, 28.8.2014 г., стр. 146).

⁴³ Директива (ЕС) 2016/797 на Европейския парламент и на Съвета от 11 май 2016 г. относно оперативната съвместимост на железопътната система в рамките на Европейския съюз (ОВ L 138, 26.5.2016 г., стр. 44).

⁴⁴ Регламент (ЕС) 2018/858 на Европейския парламент и на Съвета от 30 май 2018 г. относно одобряването и надзора на пазара на моторни превозни средства и техните ремаркета, както и на системи, компоненти и отделни технически възли, предназначени за такива превозни средства, за изменение на регламенти (ЕО) № 715/2007 и (ЕО) № 595/2009 и за отмяна на Директива 2007/46/ЕО (ОВ L 151, 14.6.2018 г., стр. 1).

⁴⁵ Регламент (ЕС) 2018/1139 на Европейския парламент и на Съвета от 4 юли 2018 г. относно общи правила в областта на гражданското въздухоплаване и за създаването на Агенция за авиационна безопасност на Европейския съюз и за изменение на регламенти (ЕО) № 2111/2005, (ЕО) № 1008/2008, (ЕС) № 996/2010, (ЕС) № 376/2014 и на директиви 2014/30/ЕС и 2014/53/ЕС на Европейския парламент и на Съвета и за отмяна на регламенти (ЕО) № 552/2004 и (ЕО) № 216/2008 на Европейския парламент и на Съвета и Регламент (ЕИО) № 3922/91 на Съвета (ОВ L 212, 22.8.2018 г., стр. 1).

⁴⁶ Регламент (ЕС) № 2019/2144 на Европейския парламент и на Съвета от 27 ноември 2019] година относно изискванията за одобряване на типа на моторни превозни средства и техните ремаркета, както и системи, компоненти и отделни технически възли, предназначени за такива превозни средства, по отношение на тяхната обща безопасност и защитата на пътниците и уязвимите участници в движението по пътищата, за изменение на Регламент (ЕС) 2018/858 на Европейския парламент и на Съвета и за отмяна на регламенти (ЕО) № 78/2009, (ЕО) № 79/2009 и (ЕО) № 661/2009 на Европейския парламент и на Съвета и регламенти (ЕО) № 631/2009, (ЕС) № 406/2010, (ЕС) № 672/2010, (ЕС) № 1003/2010, (ЕС) № 1005/2010, (ЕС) № 1008/2010, (ЕС) № 1009/2010, (ЕС) № 19/2011, (ЕС) № 109/2011, (ЕС) № 458/2011, (ЕС) № 65/2012, (ЕС) №

изменени, за да се гарантира, че Комисията отчита — въз основа на техническата и регулаторна специфика на всеки сектор и без да има вмешателство в съществуващата уредба, оценяване на съответствието и създадените в тях механизми за прилагане и органи — задължителните изисквания за високорисковите системи с ИИ, определени в настоящия регламент, когато приема евентуални имащи отношение бъдещи делегирани актове или актове за изпълнение на основание на тях.

- (30) По отношение на системите с ИИ, които са защитни компоненти на продукти или които сами по себе си са продукти, попадащи в обхвата на определено законодателство на Съюза за хармонизация, е целесъобразно те да бъдат класифицирани като високорискови съгласно настоящия регламент, ако въпросният продукт преминава през процедура за оценяване на съответствието с орган за оценяване на съответствието като трета страна съгласно съответното законодателство на Съюза за хармонизация. Подобни продукти са по-специално машини, играчки, асансьори, оборудване и защитни системи, предназначени за използване в потенциално взривоопасна среда, радиооборудване, оборудване под налягане, оборудване за плавателни съдове за отдих, въжени линии, уреди, хранени с газово гориво, медицински изделия и медицински изделия за инвитро диагностика.
- (31) Класифицирането на дадена система с ИИ като високорискова съгласно настоящия регламент не следва непременно да означава, че продуктът, чийто защитен компонент е системата с ИИ, или самата система с ИИ като продукт, се счита за високорисков или високорискова съгласно критериите, установени в съответното законодателство на Съюза за хармонизация, приложимо за продукта. Такъв е по-специално случаят с Регламент (ЕС) 2017/745 на Европейския парламент и на Съвета⁴⁷ и Регламент (ЕС) 2017/746 на Европейския парламент и на Съвета⁴⁸, в които се предвижда оценяване на съответствието от трета страна за продукти със среден и висок риск.
- (32) Що се отнася до самостоятелните системи с ИИ, т.е. високорискови системи с ИИ, различни от тези, които са защитни компоненти на продукти или които сами по себе си са продукти, целесъобразно е те да бъдат класифицирани като високорискови, ако с оглед на предназначението си представляват висок риск от увреждане на здравето и безопасността или на основните права на хората, като се вземат предвид както сериозността на възможната вреда, така и вероятността от настъпването ѝ, и системите с ИИ се използват в някои конкретно и предварително определени области, посочени в регламента. Идентифицирането на тези системи се основава на същата методология и критерии като предвидените и за евентуални бъдещи изменения на списъка на високорисковите системи с ИИ.

130/2012, (ЕС) № 347/2012, (ЕС) № 351/2012, (ЕС) № 1230/2012 и (ЕС) № 2015/166 на Комисията (ОВ L 325, 16.12.2019 г., стр. 1).

⁴⁷ Регламент (ЕС) 2017/745 на Европейския парламент и на Съвета от 5 април 2017 г. за медицинските изделия, за изменение на Директива 2001/83/ЕО, Регламент (ЕО) № 178/2002 и Регламент (ЕО) № 1223/2009 и за отмяна на директиви 90/385/ЕИО и 93/42/ЕИО на Съвета (ОВ L 117, 5.5.2017 г., стр. 1).

⁴⁸ Регламент (ЕС) 2017/746 на Европейския парламент и на Съвета от 5 април 2017 г. за медицинските изделия за инвитро диагностика и за отмяна на Директива 98/79/ЕО и Решение 2010/227/ЕС на Комисията (ОВ L 117, 5.5.2017 г., стр. 176).

- (33) Техническите неточности на системите с ИИ, предназначени за дистанционна биометрична идентификация на физически лица, могат да доведат до предубеденост на резултатите и до дискриминация. Това обстоятелство е от особено значение, когато става въпрос за възраст, етническа принадлежност, пол или увреждания. Поради това системите за дистанционна биометрична идентификация в реално време и „екс-пост“ следва да бъдат класифицирани като високорискови. С оглед на рисковете, които поражда, и двата вида системи за дистанционна биометрична идентификация следва да подлежат на специфични изисквания относно възможностите за поддържане на записи и човешкия надзор.
- (34) Що се отнася до управлението и експлоатацията на критична инфраструктура, целесъобразно е системите с ИИ, предназначени да бъдат използвани като защитни елементи при управлението и експлоатацията на движението по пътищата и водоснабдяването, газоснабдяването, отоплението и електроенергията, да бъдат класифицирани като високорискови системи с ИИ, тъй като при тях аварията или неизправността може да изложи на риск живота и здравето на множество хора и да доведе до значителни смущения в обичайното осъществяване на социални и икономически дейности.
- (35) Системите с ИИ, използвани в образованието или професионалното обучение, по-специално за определяне на достъпа до или за насочване на лица към институции за образование и професионално обучение или за оценяване на лица чрез тестове като част от или като предварително условие за тяхното образование, следва да се считат за високорискови, тъй като могат да определят образователния и професионалния път на дадено лице и така да повлияят на възможността му да осигурява прехраната си. Когато не са правилно проектирани и използвани, тези системи могат да нарушат правото на образование и обучение, както и правото на недискриминация и да продължат да възпроизвеждат модели на дискриминация от миналото.
- (36) Системите с ИИ, използвани в областта на заетостта, управлението на работници и достъпа до самостоятелна заетост, по-специално за подбор и наемане на лица, за вземане на решения относно повишения и прекратяване на договори и за разпределяне на задачи, мониторинг или оценка на лица, които имат договорни отношения във връзка с полагане на труд, също следва да бъдат класифицирани като високорискови, тъй като тези системи могат в значителна степен да повлияят на бъдещите перспективи за професионално развитие и поминък на тези лица. Сред договорните отношения във връзка с полагане на труд следва да се включват и служителите и лицата, предоставящи услуги чрез платформи, както е посочено в работната програма на Комисията за 2021 г. Такива лица по принцип не следва да се считат за ползватели по смисъла на настоящия регламент. По време на целия процес на набиране на персонал и при оценката, повишаването или задържането на лица в договорни отношения във връзка с полагане на труд такива системи могат да продължат да възпроизвеждат съществували в миналото модели на дискриминация, например срещу жени, определени възрастови групи, хора с увреждания или хора с определен расов или етнически произход или сексуална ориентация. Системите с ИИ, използвани за следене на работата и поведението на тези лица, могат също така да засегнат техните права на защита на данните и неприкосновеност на личния живот.
- (37) Друга област, в която използването на системи с ИИ заслужава специално внимание, е достъпът до и ползването на някои основни частни и обществени услуги и ползи, необходими на хората за пълноценно участие в обществото или

за подобряване на техния стандарт на живот. По-специално системите с ИИ, използвани за оценка на кредитния рейтинг или кредитоспособността на физически лица, следва да бъдат класифицирани като високорискови системи с ИИ, тъй като те определят какъв достъп ще имат тези лица до финансови ресурси или основни услуги като жилищно настаняване, електроенергия и телекомуникационни услуги. Използваните за тази цел системи с ИИ могат да доведат до дискриминация на лица или групи и да продължат да възпроизвеждат съществували в миналото модели на дискриминация, например въз основа на расов или етнически произход, увреждания, възраст, сексуална ориентация, или да създадат нови форми на дискриминация. Като се има предвид много ограничените мащаб на въздействието и наличните алтернативи на пазара, е целесъобразно системите с ИИ, служещи за оценка на кредитоспособността и кредитен рейтинг, да бъдат освободени, когато се въвеждат в експлоатация от малки доставчици за тяхна собствена употреба. Физическите лица, които кандидатстват или получават обществено подпомагане и услуги от публични органи, обикновено зависят от тези помощи и услуги и са в уязвимо положение по отношение на отговорните органи. Ако за да се определи дали тези помощи и услуги следва да бъдат отказани, намалени, отменени или възстановени от органите, се използват системи с ИИ, същите могат да окажат значително въздействие върху материалната издръжка на тези лица и да нарушат основните им права, като правото на социална закрила, недискриминация, човешко достойнство или ефективни правни средства за защита. Поради това тези системи следва да бъдат класифицирани като високорискови. Независимо от това настоящият регламент следва да не възпрепятства разработването и използването на иновативни подходи в публичната администрация, за които по-широкото използване на съвместими и безопасни системи с ИИ би било полезно, при условие че тези системи не водят до висок риск за юридическите и физическите лица. И на последно място, системите с ИИ, използвани за задействане на службите за спешно реагиране или за определяне на приоритет по отношение на него, също следва да бъдат класифицирани като високорискови, тъй като те вземат решения в ситуации, които са изключително критични за живота и здравето на хора и за тяхното имущество.

- (38) Действията на правоприлагащите органи, включващи определени употреби на системи с ИИ, се характеризират със значителна степен на властово неравновесие и могат да доведат до наблюдение, задържане или лишаване от свобода на физическо лице, както и до други неблагоприятни въздействия по отношение на основните права, гарантирани от Хартата. По-специално, ако системата с ИИ не е обучена с висококачествени данни, не отговаря на съответните изисквания по отношение на нейната точност или надеждност или не е правилно проектирана и изпитана, преди да бъде пусната на пазара или въведена в експлоатация, тя може да избира лица по дискриминационен начин или по неправилен или несправедлив в друго отношение начин. Освен това упражняването на важни основни процесуални права, като правото на ефективни правни средства за защита и на справедлив съдебен процес, както и правото на защита и презумпцията за невиновност, би могло да бъде възпрепятствано, по-специално когато системите с ИИ не са достатъчно прозрачни, обясними и документирани. Поради това е целесъобразно да се класифицират като високорискови някои системи с ИИ, предназначени да бъдат използвани в контекста на правоприлагането, където точността, надеждността и прозрачността са особено важни за избягване на неблагоприятни въздействия,

запазване на общественото доверие и гарантиране на отчетност и ефективна правна защита. С оглед на естеството на въпросните дейности и свързаните с тях рискове високорисковите системи с ИИ следва да включват по-специално системи с ИИ, предназначени да се използват от правоприлагащите органи за индивидуални оценки на риска, полиграфи и подобни инструменти или за разкриване на емоционалното състояние на физическо лице, за откриване на дълбинни фалшификати, за оценка на надеждността на доказателства в наказателни производства, за предвиждане на извършването или повторното извършване на действително или потенциално престъпление въз основа на профилиране на физически лица или за оценяване на личностни черти и характеристики или минало престъпно поведение на физически лица или групи, за профилиране в хода на откриването, разследването или наказателно преследване на престъпления, както и за криминален анализ по отношение на физически лица. Системите с ИИ, специално предназначени да се използват за административни производства от данъчните и митническите органи, не следва да се считат за високорискови системи с ИИ, използвани от правоприлагащи органи за целите на предотвратяването, разкриването, разследването и наказателното преследване на престъпления.

- (39) Системите с ИИ, използвани в управлението на миграцията, убежището и граничния контрол, засягат хора, които често са в особено уязвимо положение и които зависят от резултата от действията на компетентните публични органи. Поради това точността, недискриминационният характер и прозрачността на системите с ИИ, използвани в тези ситуации, са особено важни, за да се гарантира зачитането на основните права на засегнатите лица, по-специално правото им на свободно движение, недискриминация, защита на личния живот и личните данни, международна закрила и добра администрация. Поради това е целесъобразно като високорискови да се класифицират системите с ИИ, предназначени да бъдат използвани от компетентните публични органи, натоварени със задачи в областта на управлението на миграцията, убежището и граничния контрол, например полиграфи и подобни инструменти или такива за разкриване на емоционалното състояние на физическо лице; за оценка на определени рискове, произтичащи от физически лица, които влизат на територията на държава членка или кандидатстват за виза или убежище; за проверка на автентичността на съответните документи на физически лица; за подпомагане на компетентните публични органи при разглеждането на молби за убежище, визи и разрешения за пребиваване и свързаните с тях жалби по отношение на целта за установяване на допустимостта на физическите лица, кандидатстващи за статут. Системите с ИИ в областта на управлението на миграцията, убежището и граничния контрол, обхванати от настоящия регламент, следва да отговарят на съответните процедурни изисквания, определени в Директива 2013/32/ЕС на Европейския парламент и на Съвета⁴⁹, Регламент (ЕО) № 810/2009 на Европейския парламент и на Съвета⁵⁰ и другото съответно законодателство.

⁴⁹ Директива 2013/32/ЕС на Европейския парламент и на Съвета от 26 юни 2013 г. относно общите процедури за предоставяне и отнемане на международна закрила (ОВ L 180, 29.6.2013 г., стр. 60).

⁵⁰ Регламент (ЕО) № 810/2009 на Европейския парламент и на Съвета от 13 юли 2009 г. за създаване на Визов кодекс на Общността (Визов кодекс) (ОВ L 243, 15.9.2009 г., стр. 1).

- (40) Някои системи с ИИ, предназначени за използване в правораздаването и при демократичните процеси, следва да бъдат класифицирани като високорискови, като се има предвид потенциално значителното им въздействие върху демокрацията, принципите на правовата държава, индивидуалните свободи, както и правото на ефективни правни средства за защита и на справедлив съдебен процес. По-специално, в отговор на рисковете от потенциална предубеденост, грешки и непрозрачност, е целесъобразно да се класифицират като високорискови системите с ИИ, предназначени да подпомагат съдебните органи при проучването и тълкуването на фактите и правото и при прилагането на му към конкретен набор от факти. Подобна класификация обаче не следва да обхваща системите с ИИ, предназначени за чисто спомагателни административни дейности, които не засягат самото правораздаване спрямо отделните случаи, като например анонимизация или псевдонимизация на съдебни решения, документи или данни, комуникация между персонала, административни задачи или разпределяне на ресурси.
- (41) Фактът, че дадена система с ИИ е класифицирана като високорискова съгласно настоящия регламент, не следва да се тълкува като указване, че използването на системата е непременно законосъобразно съгласно други актове на правото на Съюза или съгласно националното право, съвместимо с правото на Съюза, като например относно защитата на личните данни, използването на полиграфи и подобни инструменти или други системи за разпознаване на емоционалното състояние на физическите лица. Всяко такова използване следва да продължи да се извършва единствено в съответствие с приложимите изисквания, произтичащи от Хартата и от приложимите актове на вторичното право на Съюза и националното право. Настоящият регламент не следва да се разбира като предоставящ правно основание за обработването на лични данни, включително по необходимост на специални категории лични данни.
- (42) За да се ограничат рисковете за ползвателите и засегнатите лица от високорисковите системи с ИИ, пуснати на пазара или иначе въведени в експлоатация на пазара на Съюза, следва да се прилагат определени задължителни изисквания, при които се взема предвид за каква цел се използва системата и които са съобразени със системата за управление на риска, която ще бъде приложена от доставчика.
- (43) По отношение на високорисковите системи с ИИ следва да се прилагат изисквания по отношение на качеството на използваните набори от данни, техническата документация и воденето на регистри, прозрачността и предоставянето на информация на ползвателите, човешкия надзор, надеждността, точността и киберсигурността. Тези изисквания са необходими за ефективно ограничаване на рисковете за здравето, безопасността и основните права, които могат да възникнат с оглед на предназначението на системата, и когато не съществуват други разумни, по-малко ограничителни мерки за търговията, като по този начин се избягват необосновани ограничения на търговията.
- (44) Високото качество на данните е от съществено значение за функционирането на много системи с ИИ, особено когато се използват техники, включващи обучение на модели, с цел да се гарантира, че високорисковата система с ИИ функционира по предназначение и по безопасен начин и не води до дискриминация, забранена от правото на Съюза. Висококачествените набори от данни за обучение, признаване и изпитване изискват прилагането на подходящи практики за

мощно и непосредствено управление на данните. Наборите от данни за обучението, признаването и изпитването следва да бъдат достатъчно подходящи, представителни, без грешки и пълни с оглед на предназначението на системата. Те следва също така да притежават подходящи статистически свойства, включително по отношение на лицата или групите лица, за които е предназначена да се използва високорисковата система с ИИ. По-специално, при обучението, признаването и изпитването на наборите от данни следва да се вземат предвид, доколкото това се изисква с оглед на предназначението им, особеностите, характеристиките или елементите, които са специфични за конкретната географска, поведенческа или функционална среда или контекст, в които системата с ИИ е предназначена да бъде използвана. За да се защитят правата на други лица от евентуална дискриминацията вследствие на предубеденост на системите с ИИ, доставчиците следва да могат да обработват и специални категории лични данни като въпрос от значителен обществен интерес, за да се гарантира наблюдението, откриването и коригирането на случаите на предубеденост на високорисковите системи с ИИ.

- (45) За разработването на високорискови системи с ИИ определени участници, като например доставчици, нотифицирани органи и други имащи отношение субекти, като например центрове за цифрови иновации, съоръжения за експериментирание и изпитване и научни изследователи, следва да имат достъп до и да използват висококачествени набори от данни в своите области на дейност, които са свързани с настоящия регламент. Общите европейски пространства на данни, създадени от Комисията, и улесняването на обмена на данни между предприятията и с държавните органи в името на обществен интерес ще бъдат от основно значение за осигуряването на надежден, отговорен и недискриминационен достъп до висококачествени данни за обучението, признаването и изпитването на системите с ИИ. Например в областта на здравеопазването европейското пространство на здравни данни ще улесни недискриминационния достъп до здравни данни и обучението на алгоритми на изкуствен интелект въз основа на тези набори от данни по сигурен, навременен, прозрачен и надежден начин, при който се опазва неприкосновеността на личния живот, и при подходящо институционално управление. Съответните компетентни органи, включително секторните органи, които предоставят или подпомагат достъпа до данни, могат също така да подкрепят предоставянето на висококачествени данни за обучението, признаването и изпитването на системите с ИИ.
- (46) Наличието на информация за това как са били разработени високорисковите системи с ИИ и как функционират през целия си жизнен цикъл е от съществено значение при проверката на съответствието с изискванията по настоящия регламент. Това изисква съхраняването на записи и наличието на техническа документация, съдържаща информация, която е необходима за оценяване на съответствието на системата с ИИ с приложимите изисквания. Тази информация следва да включва общите характеристики, възможностите и ограниченията на системата, използваните алгоритми, данни и процеси за обучение, изпитване и признаване, както и документация за съответната система за управление на риска. Техническата документация следва да се актуализира.
- (47) За да се преодолее липсата на прозрачност, която може да направи някои системи с ИИ неразбираеми или твърде сложни за физическите лица, за високорисковите системи с ИИ следва да се изисква определена степен на

прозрачност. Ползвателите следва да могат да тълкуват изходните данни на системата и да я използват по подходящ начин. Поради това високорисковите системи с ИИ следва да бъдат придружени от съответната документация и инструкции за употреба и да включват кратка и ясна информация, включително във връзка с възможните рискове за основните права и рисковете от дискриминация, когато е целесъобразно.

- (48) Високорисковите системи с ИИ следва да бъдат проектирани и разработени по такъв начин, че физическите лица да могат да следят тяхното функциониране. За тази цел доставчикът на системата следва да определи подходящи мерки за човешки надзор преди пускането ѝ на пазара или въвеждането ѝ в експлоатация. По-специално, когато е целесъобразно, тези мерки следва да гарантират, че системата е подложена на вградени оперативни ограничения, които не могат да бъдат заобиколени от самата система, и че тя отговаря на човека оператор, както и че физическите лица, на които е възложен човешкият надзор, разполагат с необходимата компетентност, обучение и правомощия за изпълнение на тази роля.
- (49) Високорисковите системи с ИИ следва да функционират стабилно през целия си жизнен цикъл и да отговарят на подходящо ниво на точност, надеждност и киберсигурност в съответствие с общопризнатото съвременно техническо равнище. Нивото на точност и показателите за точност следва да се съобщават на ползвателите.
- (50) Техническата надеждност е ключово изискване за високорисковите системи с ИИ. Те следва да бъдат устойчиви срещу рискове, свързани с ограниченията на системата (напр. грешки, дефекти, несъответствия, неочаквани ситуации), както и срещу злонамерени намеси, които могат да застрашат сигурността на системата с ИИ и да доведат до вредно или друго нежелателно поведение. Липсата на защита срещу тези рискове може да повлияе на безопасността или да се отрази отрицателно на основните права, например поради неправилни решения или погрешни или засегнати от предубеждения резултати, генерирани от системата с ИИ.
- (51) Киберсигурността играе решаваща роля, за да се гарантира, че системите с ИИ са устойчиви на опити за промяна на тяхното използване, поведение или ефективност или за компрометиране на техните свойства, свързани със сигурността, от злонамерени трети страни, които се възползват от уязвимостта на системата. Кибератаките срещу системи с ИИ могат да засегнат специфични за ИИ ресурси, като например набори от обучителни данни (напр. чрез „отравяне на данните“) или обучени модели (напр. чрез „враждебни атаки“), или да използват слабите места в цифровите ресурси на системата с ИИ или в основната ИКТ инфраструктура. За да се гарантира ниво на киберсигурност, съобразено с рисковете, доставчиците на високорисковите системи с ИИ следва да предприемат подходящи мерки, като отчитат надлежно и основната ИКТ инфраструктура.
- (52) Като част от законодателството на Съюза за хармонизация на правилата, приложими за пускането на пазара, въвеждането в експлоатация и използването на високорисковите системи с ИИ, следва да бъдат установени в съответствие с Регламент (ЕО) № 765/2008 на Европейския парламент и на Съвета за

определяне на изискванията за акредитация и надзор на пазара във връзка с предлагането на пазара на продукти⁵¹, Решение № 768/2008/ЕО на Европейския парламент и на Съвета относно обща рамка за предлагането на пазара на продукти⁵² и Регламент (ЕС) 2019/1020 на Европейския парламент и на Съвета относно надзора на пазара и съответствието на продуктите⁵³ („нова законодателна рамка за предлагането на продукти на пазара“).

- (53) Целесъобразно е конкретно физическо или юридическо лице, определено като доставчик, да поеме отговорността за пускането на пазара или въвеждането в експлоатация на дадена високорискова система с ИИ, независимо дали това физическо или юридическо лице е проектирало или разработило системата.
- (54) Доставчикът следва да създаде стабилна система за управление на качеството, да гарантира изпълнението на изискваната процедура за оценяване на съответствието, да изготви съответната документация и да създаде надеждна система за мониторинг след пускането на пазара. Публичните органи, които пускат в експлоатация високорискови системи с ИИ за свое собствено ползване, могат да приемат и прилагат правилата за системата за управление на качеството като част от приетата на национално или регионално равнище система за управление на качеството, по целесъобразност, като вземат предвид особеностите на сектора и компетентностите и организацията на въпросния публичен орган.
- (55) Когато високорискова система с ИИ, която е защитен компонент на продукт, обхванат от съответното секторно законодателство по новата законодателна рамка, не е пусната на пазара или не е въведена в експлоатация независимо от продукта, производителя на крайния продукт, както е определен в съответните разпоредби на новата законодателна рамка, следва да спазва задълженията на доставчика, установени в настоящия регламент, и по-специално да гарантира, че системата с ИИ, вградена в крайния продукт, отговаря на изискванията на настоящия регламент.
- (56) За да се даде възможност за прилагането на настоящия регламент и за да се създадат условия на равнопоставеност за операторите, както и предвид различните форми на предоставяне на цифрови продукти, е важно да се гарантира, че при всички обстоятелства установено в Съюза лице може да предостави на органите цялата необходима информация относно съответствието на дадена система с ИИ. Следователно, когато даден вносител не може да бъде идентифициран, преди да предоставят неговите системи на пазара на Съюза, доставчиците, установени извън Съюза, чрез писмено пълномощно определят упълномощен представител, който е установен в Съюза.

⁵¹ Регламент (ЕО) № 765/2008 на Европейския парламент и на Съвета от 9 юли 2008 г. за определяне на изискванията за акредитация и надзор на пазара във връзка с предлагането на пазара на продукти и за отмяна на Регламент (ЕИО) № 339/93 (ОВ L 218, 13.8.2008 г., стр. 30).

⁵² Решение № 768/2008/ЕО на Европейския парламент и на Съвета от 9 юли 2008 г. относно обща рамка за предлагането на пазара на продукти и за отмяна на Решение 93/465/ЕИО на Съвета (ОВ L 218, 13.8.2008 г., стр. 82).

⁵³ Регламент (ЕС) 2019/1020 на Европейския парламент и на Съвета от 20 юни 2019 г. относно надзора на пазара и проверките на съответствието на продуктите и за изменение на Директива 2004/42/ЕО и регламенти (ЕО) № 765/2008 и (ЕС) № 305/2011 (текст от значение за ЕИП)(ОВ L 169, 25.6.2019 г., стр. 1—44).

- (57) В съответствие с принципите на новата законодателна рамка следва да бъдат определени конкретни задължения за съответните икономически оператори, като например вносители и дистрибутори, за да се гарантира правната сигурност и да се улесни спазването на регулаторните изисквания от съответните оператори.
- (58) Предвид естеството на системите с ИИ и евентуалните рискове за безопасността и основните права, свързани с тяхното използване, включително по отношение на необходимостта да се гарантира подходящо наблюдение на работата на дадена система с ИИ в реални условия, е целесъобразно да се определят конкретни отговорности за ползвателите. Те следва по-специално да използват високорисковите системи с ИИ в съответствие с инструкциите за употреба, а също така следва да се предвидят някои други задължения по отношение на наблюдението на функционирането на системите с ИИ и по отношение на воденето на документация, когато е целесъобразно.
- (59) Уместно е да се предположи, че ползвателят на системата с ИИ ще е физическото или юридическото лице, публичният орган, агенцията или друг орган, под чието правомощие се експлоатира системата с ИИ, освен когато тя се използва в рамките на лична непрофесионална дейност.
- (60) С оглед на сложността на веригата за създаване на стойност в областта на изкуствения интелект съответните трети страни, по-специално тези, които участват в продажбата и доставката на софтуер, софтуерни инструменти и компоненти, предварително обучени модели и данни или доставчиците на мрежови услуги, следва да си сътрудничат адекватно с доставчиците и ползвателите, за да могат те да изпълняват задълженията си по настоящия регламент, както и с компетентните органи, посочени съгласно настоящия регламент.
- (61) Стандартизацията следва да играе ключова роля за предоставянето на технически решения на доставчиците, за да се гарантира спазването на настоящия регламент. Съответствието с хармонизираните стандарти, определени в Регламент (ЕС) № 1025/2012 на Европейския парламент и на Съвета⁵⁴, следва да бъде средство за доказване на спазването на изискванията на настоящия регламент от доставчиците. Комисията обаче би могла да приеме общи технически спецификации в области, в които не съществуват хармонизирани стандарти или те са недостатъчни.
- (62) За да се гарантира високо ниво на надеждност на високорисковите системи с ИИ, те следва да подлежат на оценяване на съответствието преди пускането им на пазара или въвеждането им в експлоатация.
- (63) За да се сведе до минимум тежестта за операторите и да се избегне всякакво възможно дублиране, за високорисковите системи с ИИ, свързани с продукти, които са обхванати от съществуващото законодателство на Съюза за хармонизация съгласно подхода на новата законодателна рамка, е целесъобразно

⁵⁴ Регламент (ЕС) № 1025/2012 на Европейския парламент и на Съвета от 25 октомври 2012 г. относно европейската стандартизация, за изменение на директиви 89/686/ЕИО и 93/15/ЕИО на Съвета и на директиви 94/9/ЕО, 94/25/ЕО, 95/16/ЕО, 97/23/ЕО, 98/34/ЕО, 2004/22/ЕО, 2007/23/ЕО, 2009/23/ЕО и 2009/105/ЕО на Европейския парламент и на Съвета и за отмяна на Решение 87/95/ЕИО на Съвета и на Решение № 1673/2006/ЕО на Европейския парламент и на Съвета (ОВ L 316, 14.11.2012 г., стр. 12).

съответствието на тези системи с изискванията на настоящия регламент да се оценява като част от оценяването на съответствието, което вече е предвидено съгласно посоченото законодателство. Следователно приложимостта на изискванията на настоящия регламент не следва да засяга специфичната логика, методология или обща структура за оценяване на съответствието съгласно съответното специфично законодателство по новата законодателна рамка. Този подход е напълно отразен във взаимодействието между настоящия регламент и [Регламента относно машините]. Докато рисковете за безопасността на системите с ИИ, гарантиращи функциите за безопасност в машините, са обхванати от изискванията на настоящия регламент, някои специфични изисквания в [Регламента относно машините] ще гарантират безопасното интегриране на системата с ИИ в цялата машина, така че да не се излага на риск безопасността на машината като цяло. В [Регламента относно машините] се прилага същото определение за система с ИИ като в настоящия регламент.

- (64) Като се има предвид, че професионалните сертифициращи органи преди пускането на пазара притежават по-широк опит в областта на безопасността на продуктите, както и предвид различното естество на свързаните с тези продукти рискове, е целесъобразно да се ограничи, поне в началната фаза на прилагане на настоящия регламент, приложното поле на оценяването на съответствието от трета страна за високорисковите системи с ИИ, различни от свързаните с продукти. Поради това оценяването на съответствието на такива системи следва като общо правило да се извършва от доставчика на негова отговорност, с единственото изключение на системите с ИИ, предназначени за дистанционна биометрична идентификация на лица, за които следва да се предвиди участието на нотифициран орган в оценяването на съответствието, доколкото тези системи не са забранени.
- (65) С цел извършване на оценяване на съответствието от трета страна за системи с ИИ, предназначени да се използват за дистанционна биометрична идентификация на лица, националните компетентни органи следва да определят съгласно настоящия регламент нотифицираните органи, при условие че последните отговарят на набор от изисквания, по-специално относно независимостта, компетентността и отсъствието на конфликти на интереси.
- (66) В съответствие с общоприетото понятие за съществено изменение за продукти, регулирани от законодателството на Съюза за хармонизация, е целесъобразно дадена система с ИИ да бъде подлагана на ново оценяване на съответствието всеки път, когато настъпи промяна, която може да засегне съответствието на системата с настоящия регламент, или когато предназначението на системата се промени. Освен това по отношение на системите с ИИ, които продължават да се обучават след пускането им на пазара или въвеждането им в експлоатация (т.е. автоматично адаптират начина, по който се изпълняват функциите), е необходимо да се предвидят правила, с които се установява дали промените в алгоритъма и неговите показатели, които са били предварително определени от доставчика и оценени към момента на оценяването на съответствието, не следва да се приемат като съществено изменение.
- (67) Високорисковите системи с ИИ следва да носят маркировката „СЕ“, указваща тяхното съответствие с настоящия регламент с цел свободно движение в рамките на вътрешния пазар. Държавите членки не следва да създават необосновани пречки пред пускането на пазара или въвеждането в експлоатация на

високорискови системи с ИИ, които съответстват на изискванията, предвидени в настоящия регламент, и носят маркировката „СЕ“.

- (68) При определени условия спешното осигуряване на иновативни технологии може да бъде от решаващо значение за здравето и безопасността на хората и за обществото като цяло. Поради това е целесъобразно по изключителни причини, свързани с обществената сигурност или защитата на живота и здравето на физическите лица и защитата на индустриалната и търговската собственост, държавите членки да могат да разрешават пускането на пазара или въвеждането в експлоатация на системи с ИИ, които не са преминали оценяване на съответствието.
- (69) С цел да се улесни работата на Комисията и на държавите членки в областта на изкуствения интелект, както и за да се повиши прозрачността пред обществеността, от доставчиците на високорискови системи с ИИ, различни от свързаните с продукти, попадащи в обхвата на съответното действащо законодателство на Съюза за хармонизация, следва да се изисква да регистрират своята високорискова система с ИИ в база данни на ЕС, която ще бъде създадена и управлявана от Комисията. Комисията ще бъде администратор на тази база данни в съответствие с Регламент (ЕС) 2018/1725 на Европейския парламент и на Съвета⁵⁵. За да се гарантира цялостна готовност на базата данни при нейното въвеждане, процедурата по създаване на базата данни следва да включва изготвянето на функционални спецификации от Комисията и независим одитен доклад.
- (70) Някои системи с ИИ, предназначени да взаимодействат с физически лица или да генерират съдържание, могат да породят специфични рискове от фалшификация или измама, независимо дали отговарят на критериите за високорискови системи или не. Поради това при определени обстоятелства използването на тези системи следва да подлежи на специфични задължения за прозрачност, без да се засягат изискванията и задълженията за високорискови системи с ИИ. По-специално физическите лица следва да бъдат уведомявани, че взаимодействат със система с ИИ, освен ако това не е очевидно от обстоятелствата и контекста на използване. Освен това физическите лица следва да бъдат уведомявани, когато са в контакт със система за разпознаване на емоции или със система за биометрична категоризация. Тази информация и уведомленията следва да се предоставят в достъпни формати за хората с увреждания. Освен това ползвателите на система с ИИ за генериране или обработка на изображения, аудио или видео съдържание, които до голяма степен наподобяват съществуващи лица, места или събития и навярно някой би приел за автентични, са задължени да разкрият, че съдържанието е било изкуствено създадено или обработено, като обозначат подобаващо продукта от работата на изкуствения интелект и разкрият неговия изкуствен произход.
- (71) Изкуственият интелект е бързо развиваща се съвкупност от технологии, която изисква нови форми на регулаторен надзор и безопасно пространство за експериментиране, като същевременно се гарантира отговорното новаторство и

⁵⁵ 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).

интегрирането на подходящи предпазни мерки и мерки за ограничаване на риска. За да се гарантира благоприятна за иновациите, ориентирана към бъдещето и стабилна правна рамка, националните компетентни органи от една или повече държави членки следва да бъдат насърчавани да създават регулаторни лаборатории за изкуствен интелект, за да се улесни разработването и изпитването на иновативни системи с ИИ под строг регулаторен надзор, преди тези системи да бъдат пуснати на пазара или въведени в експлоатация по друг начин.

- (72) Целите на регулаторните лаборатории следва да бъдат: насърчаване на иновациите в областта на ИИ чрез създаване на контролирана среда за експериментирание и изпитване във фазата на разработване и преди пускането на пазара, с цел да се гарантира съответствието на иновативните системи с ИИ с настоящия регламент и други съответни законодателни актове на Съюза и на държавите членки; повишаване на правната сигурност за новаторите и надзора и разбирането от страна на компетентните органи на възможностите, нововъзникващите рискове и въздействието на използването на ИИ, както и ускоряване на достъпа до пазарите, включително чрез премахване на пречките пред малките и средните предприятия (МСП) и стартиращите предприятия. За да се гарантира еднакво прилагане в целия Съюз и икономии от мащаба, е целесъобразно да се установят общи правила за прилагането на регулаторните лаборатории и рамка за сътрудничество между съответните органи, участващи в надзора на лабораториите. В съответствие с член 6, параграф 4 от Регламент (ЕС) 2016/679 и член 6 от Регламент (ЕС) 2018/1725 и без да се засяга член 4, параграф 2 от Директива (ЕС) 2016/680, настоящият регламент следва да предостави правното основание за използването на събирани за други цели лични данни за разработването на някои системи с ИИ в обществен интерес в рамките на регулаторната лаборатория за ИИ. Участниците в регулаторната лаборатория следва да осигурят подходящи гаранции и да си сътрудничат с компетентните органи, включително като следват техните насоки и действат експедитивно и добросъвестно, за да ограничат всички сериозни рискове за безопасността и основните права, които могат да се проявят по време на разработването и експериментирането в лабораторията. Поведението на участниците в регулаторната лаборатория следва да се вземе предвид, когато компетентните органи вземат решение дали да наложат административна глоба съгласно член 83, параграф 2 от Регламент 2016/679 и член 57 от Директива 2016/680.
- (73) С цел насърчаване и защита на иновациите е важно да се обърне специално внимание на интересите на малките доставчици и ползвателите на системи с ИИ. За тази цел държавите членки следва да разработят инициативи, насочени към тези оператори, включително за повишаване на осведомеността и съобщаването на информация. Освен това при определянето на таксите за оценяване на съответствието се вземат предвид специфичните интереси и нужди на малките доставчици. Разходите за превод, свързани със задължителната документация и комуникацията с органите, могат да представляват значителни разходи за доставчиците и другите оператори, особено за по-малките. Държавите членки следва по възможност да гарантират, че един от езиците, определени и приети от тях за съответната документация на доставчиците и за комуникация с операторите, е език, който в значителна степен се разбира от възможно най-голям брой трансгранични ползватели.

- (74) За да се сведат до минимум рисковете за изпълнението, произтичащи от липсата на знания и експертен опит на пазара, както и за да се улесни спазването от страна на доставчиците и нотифицираните органи на задълженията им по настоящия регламент, платформата за ИИ по заявка, европейските цифрови иновационни центрове и механизмите за изпитване и експериментирание, създадени от Комисията и държавите членки на национално равнище или на равнище ЕС, следва по възможност да допринасят за прилагането на настоящия регламент. В рамките на своята мисия и области на компетентност те могат да предоставят по-специално техническа и научна подкрепа на доставчиците и нотифицираните органи.
- (75) Целесъобразно е Комисията да улеснява, доколкото е възможно, достъпа до съоръжения за изпитване и експериментирание на органи, групи или лаборатории, създадени или акредитирани съгласно съответното законодателство на Съюза за хармонизация, които изпълняват задачи в контекста на оценяването на съответствието на продукти или изделия, попадащи в обхвата на посоченото законодателство на Съюза за хармонизация. Такъв е по-специално случаят с експертните групи, специализираните лаборатории и референтните лаборатории в областта на медицинските изделия съгласно Регламент (ЕС) 2017/745 и Регламент (ЕС) 2017/746.
- (76) За да се улесни гладкото, ефективно и хармонизирано прилагане на настоящия регламент, следва да се създаде Европейски съвет по изкуствен интелект. Той следва да отговаря за редица консултативни задачи, включително да издава становища, препоръки, съвети или насоки по въпроси, свързани с прилагането на настоящия регламент, включително относно техническите спецификации или съществуващите стандарти във връзка с изискванията, установени в настоящия регламент, и да консултира и подпомага Комисията по конкретни въпроси, свързани с изкуствения интелект.
- (77) Държавите членки играят ключова роля в прилагането и изпълнението на настоящия регламент. Във връзка с това всяка държава членка следва да определи един или повече национални компетентни органи за целите на надзора върху прилагането и изпълнението на настоящия регламент. С цел да се повиши ефективността на организацията от страна на държавите членки и да се създаде официално звено за контакт с обществеността и други партньори на равнището на държавите членки и на равнището на Съюза, във всяка държава членка за национален надзорен орган следва да бъде определен по един национален орган.
- (78) За да се гарантира, че доставчиците на високорискови системи с ИИ могат да вземат предвид опита от използването на високорискови системи с ИИ, за да подобряват своите системи и процеса на проектиране и разработване, или че могат своевременно да предприемат евентуални коригиращи действия, всички доставчици следва да разполагат със система за мониторинг след пускането на пазара. Тази система е от ключово значение и за това да се гарантира, че възможните рискове, произтичащи от системите с ИИ, които продължават да се обучават след пускането им на пазара или въвеждането им в експлоатация, могат да бъдат преодолені по-ефикасно и своевременно. В този контекст от доставчиците следва също така да се изисква да разполагат със система за докладване до съответните органи за всякакви сериозни инциденти или нарушения на националното право и правото на Съюза за защита на основните права, произтичащи от използването на техните системи с ИИ.

- (79) С цел да се гарантира подходящо и ефективно прилагане на изискванията и задълженията, установени с настоящия регламент, а именно законодателството на Съюза за хармонизация, системата за надзор на пазара и съответствието на продуктите, установена с Регламент (ЕС) 2019/1020, следва да се прилага в своята цялост. Когато това е необходимо за изпълнението на техните правомощия, националните публични органи или структури, които упражняват надзор върху прилагането на правото на Съюза за защита на основните права, включително органите по въпросите на равенството, следва също да имат достъп до всяка документация, изготвена съгласно настоящия регламент.
- (80) Законодателството на Съюза в областта на финансовите услуги включва вътрешни правила за общо управление и за управление на риска и изисквания, които са приложими за регулираните финансови институции в процеса на предоставяне на тези услуги, включително когато те използват системи с ИИ. За да се гарантира съгласувано прилагане и изпълнение на задълженията по настоящия регламент и на съответните правила и изисквания на законодателството на Съюза в областта на финансовите услуги, органите, отговарящи за надзора и изпълнението на законодателството в областта на финансовите услуги, включително, когато е приложимо, Европейската централна банка, следва да бъдат определени за компетентни органи за целите на надзора на прилагането на настоящия регламент, включително за дейностите по надзор на пазара по отношение на системите с ИИ, предоставяни или използвани от регулирани и контролирани финансови институции. За да се подобри допълнително съгласуваността между настоящия регламент и правилата, приложими за кредитните институции, регулирани съгласно Директива 2013/36/ЕС на Европейския парламент и на Съвета⁵⁶, е целесъобразно също така процедурата за оценяване на съответствието и някои от процедурните задължения на доставчиците във връзка с управлението на риска, наблюдението след пускането на пазара и документирането да бъдат включени в съществуващите задължения и процедури съгласно Директива 2013/36/ЕС. За да се избегне припокриване, следва да се предвидят и ограничени дерогации във връзка със системата за управление на качеството на доставчиците и задължението за наблюдение, наложено на ползвателите на високорискови системи с ИИ, доколкото те се прилагат за кредитните институции, регулирани от Директива 2013/36/ЕС.
- (81) Разработването на системи с ИИ, различни от високорискови системи с ИИ, в съответствие с изискванията на настоящия регламент може да доведе до по-широко внедряване на надежден изкуствен интелект в Съюза. Доставчиците на невисокорискови системи с ИИ следва да бъдат насърчавани да създават кодекси за поведение, предназначени да насърчават доброволното прилагане на задължителните изисквания, приложими за високорисковите системи с ИИ. Доставчиците следва също така да бъдат насърчавани да прилагат на доброволна основа допълнителни изисквания, свързани например с екосъобразността на системите с ИИ, тяхната достъпност за хора с увреждания, участието на заинтересованите страни в тяхното проектиране и разработване и културно-

⁵⁶ Директива 2013/36/ЕС на Европейския парламент и на Съвета от 26 юни 2013 г. относно достъпа до осъществяването на дейност от кредитните институции и относно пруденциалния надзор върху кредитните институции и инвестиционните посредници, за изменение на Директива 2002/87/ЕО и за отмяна на директиви 2006/48/ЕО и 2006/49/ЕО (ОВ L 176, 27.6.2013 г., стр. 338).

личностното разнообразие на екипите от разработчици. Комисията може да разработва инициативи, включително от секторно естество, за да улесни намаляването на техническите пречки, които възпрепятстват трансграничния обмен на данни за разработването на ИИ, включително относно инфраструктурата за достъп до данни, семантичната и техническата оперативна съвместимост на различните видове данни.

- (82) Важно е системите с ИИ, свързани с продукти, които не са високорискови в съответствие с настоящия регламент и поради това не е задължително да отговарят на изискванията, посочени в настоящия регламент, да бъдат безопасни при пускането им на пазара или въвеждането им в експлоатация. В услуга на тази цел Директива 2001/95/ЕО на Европейския парламент и на Съвета⁵⁷ ще се прилага като предпазна мрежа.
- (83) За да се гарантира надеждно и конструктивно сътрудничество между компетентните органи на равнището на Съюза и на национално равнище, всички страни, участващи в прилагането на настоящия регламент, следва да зачитат поверителността на информацията и данните, получавани при изпълнението на техните задачи.
- (84) Държавите членки следва да предприемат всички необходими мерки, за да гарантират прилагането на разпоредбите на настоящия регламент, включително чрез установяването на ефективни, пропорционални и възпиращи санкции за тяхното нарушаване. За някои специфични нарушения държавите членки следва да вземат предвид допустимите отклонения и критериите, определени в настоящия регламент. Европейският надзорен орган по защита на данните следва да има правомощията да налага административни глоби на институциите, агенциите и органите на Съюза, попадащи в обхвата на настоящия регламент.
- (85) С цел да се гарантира, че, когато е необходимо, регулаторната рамка може да бъде адаптирана, на Комисията следва да бъде делегирано правомощието да приема актове в съответствие с член 290 от ДФЕС за изменение на посочените в приложение I техники и подходи за определяне на системите с ИИ, законодателството на Съюза за хармонизация, посочено в приложение II, високорисковите системи с ИИ, изброени в приложение III, разпоредбите относно техническата документация, изброени в приложение IV, съдържанието на декларацията за съответствие с изискванията на ЕС в приложение V, разпоредбите относно процедурите за оценяване на съответствието в приложения VI и VII и разпоредбите за установяване на високорисковите системи с ИИ, за които се прилага процедурата за оценяване на съответствието въз основа на оценката на системата за управление на качеството и оценката на техническата документация. От особена важност е по време на подготвителната си работа Комисията да проведе подходящи консултации, включително на експертно равнище, и тези консултации да бъдат проведени в съответствие с принципите, определени в Междунституционалното споразумение от 13 април 2016 г. за по-добро законотворчество⁵⁸. По-специално, с цел осигуряване на равно участие при подготовката на делегираните актове, Европейският парламент и Съветът получават всички документи едновременно с експертите от

⁵⁷ Директива 2001/95/ЕО на Европейския парламент и на Съвета от 3 декември 2001 г. относно общата безопасност на продуктите (ОВ L 11, 15.1.2002 г., стр. 4).

⁵⁸ ОВ L 123, 12.5.2016 г., стр. 1.

държавите членки, като техните експерти получават систематично достъп до заседанията на експертните групи на Комисията, занимаващи се с подготовката на делегираните актове.

- (86) За да се гарантират еднакви условия за изпълнение на настоящия регламент, на Комисията следва да бъдат предоставени изпълнителни правомощия. Тези правомощия следва да бъдат упражнявани в съответствие с Регламент (ЕС) № 182/2011 на Европейския парламент и на Съвета⁵⁹.
- (87) Доколкото целта на настоящия регламент не може да бъде постигната в достатъчна степен от държавите членки, а поради мащаба или последиците на действието може да бъде по-добре постигната на равнището на Съюза, Съюзът може да приеме мерки в съответствие с принципа на субсидиарност, уреден в член 5 от Договора за Европейския съюз. В съответствие с принципа на пропорционалност, уреден в същия член, настоящият регламент не надхвърля необходимото за постигането на тази цел.
- (88) Настоящият регламент следва да се прилага от ... [*до Службата за публикации – моля, въведете датата, посочена в член 85*]. Същевременно инфраструктурата, свързана с управлението и системата за оценяване на съответствието, следва да започне да функционира преди тази дата, поради което разпоредбите относно нотифицираните органи и структурата на управление следва да се прилагат от ... [*до Службата за публикации – моля, въведете датата – три месеца след влизането в сила на настоящия регламент*]. Освен това държавите членки следва да определят и изпратят до Комисията правилата относно санкциите, включително административните глоби, и да гарантират, че те се прилагат правилно и ефективно до началната дата на прилагане на настоящия регламент. Поради това разпоредбите относно санкциите следва да се прилагат от [*до Службата за публикации – моля, въведете датата – дванадесет месеца след влизането в сила на настоящия регламент*].
- (89) В съответствие с член 42, параграф 2 от Регламент (ЕО) № 2018/1725 беше проведена консултация с Европейския надзорен орган по защита на данните и Европейския комитет по защита на данните, които представиха становище на [...] г.,

ПРИЕХА НАСТОЯЩИЯ РЕГЛАМЕНТ:

ДЯЛ I

ОБЩИ РАЗПОРЕДБИ

Член 1 *Предмет*

С настоящия регламент се определят:

⁵⁹ Регламент (ЕС) № 182/2011 на Европейския парламент и на Съвета от 16 февруари 2011 г. за установяване на общите правила и принципи относно реда и условията за контрол от страна на държавите членки върху упражняването на изпълнителните правомощия от страна на Комисията (ОВ L 55, 28.2.2011 г., стр. 13).

- а) хармонизирани правила за пускането на пазара, въвеждането в експлоатация и използването на системи с изкуствен интелект („системи с ИИ“) в Съюза;
- б) забрани на някои практики в областта на изкуствения интелект;
- в) специфични изисквания за високорисковите системи с ИИ и задължения за операторите на такива системи;
- г) хармонизирани правила за прозрачност за системите с ИИ, предназначени да взаимодействат с физически лица, за системи за разпознаване на емоции и системите за биометрично категоризиране и за системите с ИИ, използвани за генериране или манипулиране на образно, аудио или видео съдържание;
- д) правила за наблюдение и надзор на пазара.

Член 2 *Обхват*

1. Настоящият регламент се прилага по отношение на:
 - а) доставчиците, които пускат на пазара или въвеждат в експлоатация системи с ИИ в Съюза, независимо дали тези доставчици са установени в Съюза или в трета държава;
 - б) ползвателите на системи с ИИ, намиращи се на територията на Съюза;
 - в) доставчиците и ползвателите на системи с ИИ, намиращи се в трета държава, когато резултатът, получен от системата, се използва в Съюза.
2. За високорисковите системи с ИИ, които са защитни елементи на продукти или системи или които сами по себе си са продукти или системи, попадащи в обхвата на следните актове, се прилага само член 84 от настоящия регламент:
 - а) Регламент (ЕО) № 300/2008;
 - б) Регламент (ЕС) № 167/2013;
 - в) Регламент (ЕС) № 168/2013;
 - г) Директива 2014/90/ЕС;
 - д) Директива (ЕС) 2016/797;
 - е) Регламент (ЕС) 2018/858;
 - ж) Регламент (ЕС) 2018/1139;
 - з) Регламент (ЕС) 2019/2144.
3. Настоящият регламент не се прилага за системи с ИИ, разработени или използвани изключително за военни цели.
4. Настоящият регламент не се прилага за публични органи в трета държава, нито за международни организации, попадащи в обхвата на настоящия регламент съгласно параграф 1, когато тези органи или организации използват системи с ИИ в рамките на международни споразумения за правоприлагане и съдебно сътрудничество със Съюза или с една или повече държави членки.
5. Настоящият регламент не засяга прилагането на разпоредбите относно отговорността на междинните доставчици на услуги, определени в глава II,

раздел IV от Директива 2000/31/ЕО на Европейския парламент и Съвета ⁶⁰ [които ще бъдат заменени от съответните разпоредби на Законодателния акт за цифровите услуги].

Член 3 Определения

За целите на настоящия регламент се прилагат следните определения:

- (1) „система с изкуствен интелект“ (система с ИИ) означава софтуер, разработен с една или повече от техниките и подходите, посочени в приложение I, който може по отношение на даден набор от цели, определени от човек, да генерира резултати, като съдържание, прогнози, препоръки или решения, които оказват въздействие върху средите, с които взаимодействат;
- (2) „доставчик“ означава физическо или юридическо лице, публичен орган, агенция или друга организация, която разработва система с ИИ или която възлага разработването на система с ИИ с цел пускането ѝ на пазара или въвеждането ѝ в експлоатация със своето име или търговска марка, срещу заплащане или безплатно;
- (3) „малък доставчик“ означава доставчик, който е микро- или малко предприятие по смисъла на Препоръка 2003/361/ЕО на Комисията⁶¹;
- (4) „ползвател“ означава всяко физическо или юридическо лице, публичен орган, агенция или друга организация, които използват система с ИИ, по отношение на която имат правомощия, с изключение на случаите, когато системата с ИИ се използва в процеса на лична непрофесионална дейност;
- (5) „упълномощен представител“ означава всяко физическо или юридическо лице, установено в Съюза, което е упълномощено писмено от доставчик на система с ИИ съответно да изпълнява и извършва от негово име задълженията и процедурите, установени в настоящия регламент;
- (6) „вносител“ означава всяко физическо или юридическо лице, установено в Съюза, което пуска на пазара или въвежда в експлоатация система с ИИ, която носи името или търговската марка на физическо или юридическо лице, установено извън Съюза;
- (7) „дистрибутор“ означава всяко физическо или юридическо лице във веригата на доставки, различно от доставчика или вносителя, което предоставя система с ИИ на пазара на Съюза, без да засяга характеристиките ѝ;
- (8) „оператор“ означава доставчик, ползвател, упълномощен представител, вносител и дистрибутор;
- (9) „пускане на пазара“ означава предоставянето на система с ИИ на пазара на Съюза за първи път;

⁶⁰ Директива 2000/31/ЕО на Европейския парламент и на Съвета от 8 юни 2000 г. относно някои правни аспекти на услугите на информационното общество, и по-специално на електронната търговия на вътрешния пазар („Директива за електронната търговия“) (ОВ L 178, 17.7.2000 г., стр. 1).

⁶¹ Препоръка на Комисията от 6 май 2003 г. относно определението за микро-, малки и средни предприятия (ОВ L 124, 20.5.2003 г., стр. 36).

- (10) „предоставяне на пазара“ означава всяка доставка на система с ИИ за дистрибуция или използване на пазара на Съюза в процеса на търговска дейност, срещу заплащане или безплатно;
- (11) „въвеждане в експлоатация“ означава доставката на система с ИИ за първо използване пряко на ползвателя или за собствено използване на пазара на Съюза в съответствие с нейното предназначение;
- (12) „предназначение“ означава използването, за което е предназначена една система с ИИ от доставчика, включително специфичният контекст и условия на употреба, посочени в информацията, предоставена от доставчика в инструкциите за употреба, рекламните или търговските материали и твърдения, както и в техническата документация;
- (13) „разумно предвидима неправилна експлоатация“ е използването на система с ИИ по начин, който не е в съответствие с нейното предназначение, но който е възможно да е резултат от разумно предвидимо човешко поведение или от взаимодействие с други системи;
- (14) „защитен елемент на продукт или система“ означава компонент на продукт или система, който осигурява функция, свързана с безопасността, за този продукт или тази система или чиято неизправност или лошо функциониране поставя в опасност здравето и безопасността на хора или имущество;
- (15) „инструкции за употреба“ означава информацията, предоставена от доставчика, за да информира ползвателя по-специално за предназначението и точната употреба на дадена система с ИИ, включително за специфичните географски, поведенчески или функционални условия, в които е предвидено да се използва високорисковата система с ИИ;
- (16) „изземване на система с ИИ“ означава всяка мярка, целяща да постигне връщане на доставчика на система с ИИ, която вече е била предоставена на ползвателите;
- (17) „изтегляне на система с ИИ“ означава всяка мярка, целяща предотвратяване на дистрибутирането, представянето и предлагането на система с ИИ;
- (18) „действие на система с ИИ“ означава способността на една система с ИИ да изпълни предназначението си;
- (19) „нотифициращ орган“ означава националният орган, отговарящ за въвеждането и извършването на необходимите процедури за оценяването, определянето и нотифицирането на органи за оценяване на съответствието и за провеждането на мониторинг по отношение на тях;
- (20) „оценяване на съответствието“ означава процесът на проверка дали са изпълнени изискванията, определени в дял III, глава 2 от настоящия регламент по отношение на система с ИИ;
- (21) „орган за оценяване на съответствието“ означава орган, осъществяващ дейности по оценяване на съответствието от трета страна, включително изпитване, сертификация и контрол;
- (22) „нотифициран орган“ е орган за оценяване на съответствието, определен съгласно настоящия регламент и друго приложимо законодателство на Съюза за хармонизация;

- (23) „съществено изменение“ означава промяна в система с ИИ след пускането ѝ на пазара или въвеждането ѝ в експлоатация, която засяга съответствието на системата с ИИ с изискванията, определени в дял III, глава 2 от настоящия регламент, или води до промяна на предназначението, за което е била оценена системата с ИИ;
- (24) „маркировка за съответствие „СЕ“ („маркировка „СЕ“) означава маркировка, чрез която доставчикът указва, че дадена система с ИИ е в съответствие с изискванията, определени в дял III, глава 2 от настоящия регламент и в друго приложимо законодателство на Съюза, с което се хармонизират условията за предлагане на продукти на пазара („законодателство на Съюза за хармонизация“) и в което се предвижда нейното нанасяне;
- (25) „мониторинг след пускането на пазара“ означава всички дейности, извършвани от доставчиците на системи с ИИ с цел проактивно събиране и преглеждане на опита, натрупан от използването на системите с ИИ, които са пуснати на пазара или въвели в експлоатация, с оглед на установяване на евентуална необходимост от незабавно прилагане на корективни или превантивни действия;
- (26) „орган за надзор на пазара“ означава националният орган, извършващ дейностите и предприемащ мерките съгласно Регламент (ЕС) 2019/1020;
- (27) „хармонизиран стандарт“ означава европейски стандарт съгласно определението от член 2, параграф 1, буква в) от Регламент (ЕС) № 1025/2012;
- (28) „общи спецификации“ означава документ, който е различен от стандарт и който съдържа технически решения, даващи възможност да се постигне съответствие с определени изисквания и задължения, установени с настоящия регламент;
- (29) „обучителни данни“ означава данни, използвани за обучение на система с ИИ чрез настройка на нейните обучавани параметри, включително теглата, използвани в невронна мрежа;
- (30) „валидационни данни“ означава данни, използвани за осигуряване на оценка на обучената система с ИИ и за настройка на нейните необучавани параметри и на обучителния ѝ процес с цел, наред с другото, да се предотврати прекомерно нагаждане; валидационният набор от данни може да бъде отделен набор от данни или част от обучителния набор от данни чрез фиксирано или променливо разделяне на данните;
- (31) „изпитвателни данни“ означава данни, използвани за извършване на независима оценка на обучената и валидирана система с ИИ с цел потвърждение на очакваното действие на тази система преди пускането ѝ на пазара или въвеждането ѝ в експлоатация;
- (32) „входящи данни“ означава данни, предоставяни на система с ИИ или пряко придобивани от нея, въз основа на които системата произвежда резултат;
- (33) „биометрични данни“ означава лични данни, получени в резултат на специфично техническо обработване, които са свързани с физическите, физиологичните или поведенческите характеристики на дадено физическо лице и които позволяват или потвърждават уникалната идентификация на това физическо лице, като лицеви изображения или дактилоскопични данни;

- (34) „система за разпознаване на емоции“ означава система с ИИ, чието предназначение е да идентифицира или да прави заключения за емоциите или намеренията на физически лица на базата на техните биометрични данни;
- (35) „система за биометрично категоризиране“ означава система с ИИ с предназначение да отнася физически лица към конкретни категории, като пол, възраст, цвят на косата, цвят на очите, татуировки, етнически произход или сексуална или политическа ориентация, на базата на техните биометрични данни;
- (36) „система за дистанционна биометрична идентификация“ означава система с ИИ с предназначение идентифициране на физически лица от разстояние чрез сравняване на биометричните данни на дадено лице с биометричните данни, съдържащи се в референтна база данни, като ползвателят на системата с ИИ не знае предварително дали лицето ще присъства в нея и може да бъде идентифицирано;
- (37) „система за дистанционна биометрична идентификация в реално време“ означава система за дистанционна биометрична идентификация, при която снемането на биометрични данни, сравнението и идентификацията се осъществяват без значително забавяне. Тук се включва не само моменталното идентифициране, но и ограничени кратки забавяния с цел недопускане на заобикаляне;
- (38) „система за екс-пост дистанционна биометрична идентификация“ означава система за дистанционна биометрична идентификация, различна от система за дистанционна биометрична идентификация в реално време;
- (39) „обществено достъпно място“ означава всяко физическо място, което е достъпно за обществеността, независимо дали има евентуални условия за достъп;
- (40) „правоприлагащ орган“ означава:
- а) всеки публичен орган, който има правомощия за превенция, разследване, откриване или преследване на престъпления или за изпълнение на наказателноправни санкции, включително предохранителни мерки срещу и превенция на заплахи за обществената сигурност; или
 - б) всяка друга организация или субект, на която или на който по силата на правото на държава членка е възложено да упражнява публична власт и публични правомощия за целите на превенцията, разследването, откриването или преследването на престъпления или изпълнението на наказателноправни санкции, включително предохранителни мерки срещу и превенция на заплахи за обществената сигурност;
- (41) „правоприлагане“ означава действията, които правоприлагащите органи извършват за превенция, разследване, откриване или преследване на престъпления или за изпълнение на наказателноправни санкции, включително предохранителни мерки срещу и превенция на заплахи за обществената сигурност;
- (42) „национален надзорен орган“ означава органът, на който дадена държава членка възлага отговорността за изпълнението и прилагането на настоящия регламент, за координацията на дейностите, възложени на тази държава членка, за функцията като единно звено за контакт за Комисията и за

представяване на държавата членка в Европейския съвет по изкуствен интелект;

- (43) „национален компетентен орган“ означава националният надзорен орган, нотифициращият орган и органът за надзор на пазара;
- (44) „сериозен инцидент“ означава всеки инцидент, който пряко или косвено води, е могъл да доведе или може да доведе до някое от следните:
- а) смърт на човек или сериозно увреждане на здравето на човек, на имущество или на околната среда,
 - б) сериозно и необратимо нарушаване на управлението и действието на критична инфраструктура.

Член 4

Изменения на приложение I

На Комисията се предоставя правомощието да приема делегирани актове в съответствие с член 73 за изменение на списъка на техниките и подходите в приложение I с цел неговото актуализиране в съответствие с промените на пазара и в технологиите на базата на характеристики, които са сходни с техниките и подходите, посочени в това приложение.

ДЯЛ II

ЗАБРАНЕНИ ПРАКТИКИ В СФЕРАТА НА ИЗКУСТВЕНИЯ ИНТЕЛЕКТ

Член 5

1. Следните практики в сферата на изкуствения интелект се забраняват:
- а) пускането на пазара, въвеждането в експлоатация или използването на система с ИИ, която си служи със сублиминални техники отвъд рамките на съзнаването от човека, с цел съществено да измени поведението на дадено лице по начин, който причинява или може да причини на същото или на друго лице физически или психологически вреди;
 - б) пускането на пазара, въвеждането в експлоатация или използването на система с ИИ, която използва което и да е от уязвимите места на конкретна група лица, дължащи се на тяхната възраст, физическо или психическо увреждане, с цел съществено да измени поведението на дадено лице, принадлежащо към тази група, по начин, който причинява или може да причини на същото или на друго лице физически или психологически вреди;
 - в) пускането на пазара, въвеждането в експлоатация или използването на система с ИИ от страна на публични органи или от тяхно име с цел оценка или класифициране на надеждността на физически лица в течение на определен срок на база на тяхното социално поведение или известни или прогнозиранни лични или личностни характеристики, като социалният ранкинг води до едното или и двете от следните:

- i) увреждащо или неблагоприятно третиране на определени физически лица или на цели групи от такива лица в социални контексти, които нямат връзка с контекстите, в които първоначално са били генерирани или събрани данните;
 - ii) увреждащо или неблагоприятно третиране на определени физически лица или на цели групи от такива лица, което е неоправдано или непропорционално на тяхното социално поведение или на тежестта, която му се отдава;
- г) използването на системи за дистанционна биометрична идентификация в реално време в обществено достъпни места за целите на правоприлагането, освен ако и доколкото такова използване е строго необходимо за една от следните цели:
- i) целево издирване на конкретни потенциални жертви на престъпления, включително изчезнали деца;
 - ii) предотвратяване на конкретна, значителна и непосредствена заплаха за живота или физическата безопасност на физически лица или за терористично нападение;
 - iii) откриване, локализиране, идентифициране или преследване на извършител или заподозрян в извършването на престъпление, посочено в член 2, параграф 2 от Рамково решение 2002/584/ПВР на Съвета⁶² и наказуемо в съответната държава членка с лишаване от свобода или мярка за задържане с максимален срок не по-малко от 3 години, както е определено в законодателството на съответната държава членка.

2. При използването на системи за дистанционна биометрична идентификация в реално време в обществено достъпни места за целите на правоприлагането за която и да е от целите, посочени в параграф 1, буква г), се отчитат следните елементи:

- а) естеството на ситуацията, която води до евентуалното използване, по-специално сериозността, вероятността и мащаба на причинената вреда, ако системата не се използва;
- б) последиците от използването на системата за правата и свободите на всички засегнати лица, по-специално тежестта, вероятността и мащабът на тези последици.

Освен това използването на системи за дистанционна биометрична идентификация в реално време на обществено достъпни места за целите на правоприлагането за която и да е от целите, посочени в параграф 1, буква г), трябва да съответства на необходимите и пропорционални гаранции и условия във връзка с използването, по-специално по отношение на времевите и географските ограничения и ограниченията по отношение на лицата.

3. Що се отнася до параграф 1, буква г) и параграф 2, всяко отделно използване за целите на правоприлагането на система за дистанционна биометрична

⁶² Рамково решение 2002/584/ПВР на Съвета от 13 юни 2002 г. относно европейската заповед за арест и процедурите за предаване между държавите членки (ОВ L 190, 18.7.2002 г., стр. 1).

идентификация в реално време на обществено достъпни места подлежи на предварително разрешение, издадено от съдебен орган или от независим административен орган на държавата членка, в която ще се осъществи използването, след получаване на мотивирано искане и в съответствие с подробните правила на националното право, както е посочено в параграф 4. При надлежно обосновани спешни случаи обаче използването на системата може да започне без разрешение и разрешение да се поиска едва по време на или след използването ѝ.

Компетентният съдебен или административен орган издава разрешение само ако въз основа на обективни доказателства или ясни индикации, които са му представени, е убеден, че използването на въпросната система за дистанционна биометрична идентификация в реално време е необходимо и пропорционално за постигането на една или повече от целите, посочени в параграф 1, буква г), съгласно искането. Когато взема решение по искането, компетентният съдебен или административен орган взема предвид елементите, посочени в параграф 2.

4. Една държава членка може да реши да предвиди възможността за пълно или частично разрешаване на използването на системи за дистанционна биометрична идентификация в реално време на обществено достъпни места за целите на правоприлагането в рамките на ограниченията и при условията, изброени в параграф 1, буква г) и в параграфи 2 и 3. Тази държава членка определя в националното си законодателство необходимите подробни правила за подаване на искания за разрешенията, посочени в параграф 3, тяхното издаване, изпълнение, както и надзора по отношение на тях. В тези правила се уточнява също така по отношение на кои от целите, посочени в параграф 1, буква г), включително по отношение на кои престъпления, посочени в подточка iii) от същата разпоредба, на компетентните органи може да бъде разрешено да използват тези системи за целите на правоприлагането.

ДЯЛ III

ВИСОКОРИСКОВИ СИСТЕМИ С ИИ

ГЛАВА 1

КЛАСИФИКАЦИЯ НА ВИСОКОРИСКОВИТЕ СИСТЕМИТЕ С ИИ

Член 6

Правила за класифициране на високорисковите системи с ИИ

1. Без оглед на това дали дадена система с ИИ се пуска на пазара или се въвежда в експлоатация независимо от продуктите, посочени в букви а) и б), тази система с ИИ се счита за високорискова, когато са изпълнени следните две условия:
 - а) системата с ИИ е предназначена да се използва като защитен елемент от продукт или самата тя е продукт, попадащ в обхвата на законодателството на Съюза за хармонизация, посочено в приложение II;
 - б) продуктът, чийто защитен елемент е системата с ИИ, или самата система с ИИ като продукт трябва да премине оценяване на съответствието от

трета страна с оглед на пускането на пазара или въвеждането в експлоатация на посочения продукт в съответствие със законодателството на Съюза за хармонизация, посочено в приложение II.

2. В допълнение към високорисковите системи с ИИ, посочени в параграф 1, за високорискови се считат и системите с ИИ, посочени в приложение III.

Член 7

Изменения на приложение III

1. На Комисията се предоставя правомощието да приема делегирани актове в съответствие с член 73 за актуализиране на списъка в приложение III чрез добавяне на високорискови системи с ИИ, когато са изпълнени следните две условия:
 - а) системите с ИИ са предназначени за използване в която и да е от областите, посочени в точки 1—8 от приложение III;
 - б) системите с ИИ крият риск от увреждане на здравето и безопасността или риск от неблагоприятно въздействие върху основните права, който е — по отношение на своята сериозност и вероятност от възникване — равностоен на или по-голям от риска от увреждане или неблагоприятно въздействие, произтичащ от високорисковите системи с ИИ, които вече са посочени в приложение III.
2. Когато за целите на параграф 1 се прави оценка дали една система с ИИ крие риск от увреждане на здравето и безопасността или риск от неблагоприятно въздействие върху основните права, който е равностоен или по-голям от риска от увреждане, произтичащ от високорисковите системи с ИИ, които вече са посочени в приложение III, Комисията взема предвид следните критерии:
 - а) предназначението на системата с ИИ;
 - б) степента, до която дадена система с ИИ е била използвана или е вероятно да бъде използвана;
 - в) степента, до която използването на система с ИИ вече е причинило увреждане на здравето и безопасността или неблагоприятно въздействие върху основните права или е породило значителни опасения във връзка с настъпването на такова увреждане или неблагоприятно въздействие и за това свидетелстват доклади или документираны твърдения, представени на националните компетентни органи;
 - г) потенциалната степен на такова увреждане или неблагоприятно въздействие, по-специално по отношение на неговия интензитет и способността му да засегне множество лица;
 - д) степента, в която лицата, претърпели потенциално увреждане или неблагоприятно въздействие, зависят от резултата, получен от дадена система с ИИ, по-специално тъй като поради практически или правни причини не е възможно в разумна степен да не използват този резултат;
 - е) степента, в която лицата, претърпели потенциално увреждане или неблагоприятно въздействие, се намират в уязвимо положение по отношение на ползвателя на система с ИИ, по-специално поради

- дисбаланс на власт, познания, икономическо или социално положение или поради своята възраст;
- ж) степента, в която резултатът, получен с помощта на система с ИИ, е лесно обратим, като резултатите, които засягат здравето или безопасността на хора, няма да се считат за лесно обратими;
 - з) степента, в която в съществуващото законодателство на Съюза са предвидени:
 - i) ефективни мерки за правна защита във връзка с рисковете, произтичащи от дадена система с ИИ, с изключение на исковете за обезщетение;
 - ii) ефективни мерки за предотвратяване или значително минимизиране на тези рискове.

ГЛАВА 2

ИЗИСКВАНИЯ ПО ОТНОШЕНИЕ НА ВИСОКОРИСКОВИТЕ СИСТЕМИ С ИИ

Член 8

Съответствие с изискванията

1. Високорисковите системи с ИИ трябва да отговарят на изискванията, определени в настоящата глава.
2. При осигуряването на съответствие с тези изисквания се вземат предвид предназначението на високорисковата система с ИИ и системата за управление на риска, посочена в член 9.

Член 9

Система за управление на риска

1. Във връзка с високорисковите системи с ИИ се създава, прилага, документираща и поддържа система за управление на риска.
2. Системата за управление на риска се състои от непрекъснат процес, протичащ през целия експлоатационен срок на високорисковата система с ИИ и изискващ редовно и систематично актуализиране. Тя включва следните стъпки:
 - а) идентифициране и анализ на известните и предвидимите рискове, свързани с всяка високорискова система с ИИ;
 - б) прогноза за и оценка на рисковете, които могат да възникнат, когато високорисковата система с ИИ се използва в съответствие със своето предназначение и при условия на разумно предвидима неправилна експлоатация;
 - в) оценка на други евентуално възникващи рискове на база анализ на данните, събрани от системата за мониторинг след пускането на пазара, посочена в член 61;
 - г) приемане на подходящи мерки за управление на риска в съответствие с разпоредбите на следващите параграфи.

3. По отношение на мерките за управление на риска, посочени в параграф 2, буква г), надлежно се отчитат ефектите и възможните взаимодействия, възникващи от съчетаното прилагане на изискванията, определени в настоящата глава 2. Отчита се общопризнатото съвременно техническо равнище, включително както е отразено в съответните хармонизирани стандарти или общи спецификации.
4. Мерките за управление на риска, посочени в параграф 2, буква г), трябва да бъдат такива, че евентуалният остатъчен риск, свързан с всяка опасност, както и общият остатъчен риск на високорисковите системи с ИИ да се счита за приемлив, при условие че високорисковата система с ИИ се използва по предназначение или в условия на разумно предвидима неправилна експлоатация. Остатъчните рискове се съобщават на ползвателя.

При определянето на най-подходящите мерки за управление на риска се осигурява следното:

- а) отстраняване или намаляване на рисковете, доколкото е възможно, чрез адекватно проектиране и разработка;
- б) когато е целесъобразно, изпълнение на адекватни мерки за ограничаване и контрол по отношение на рисковете, които не могат да бъдат отстранени;
- в) предоставяне на адекватна информация съгласно член 13, по-специално по отношение на рисковете, посочени в параграф 2, буква б) от настоящия член, и където е целесъобразно, обучение на ползвателите.

При отстраняването или намаляването на рисковете, свързани с използването на високорисковата система с ИИ, се отчитат надлежно техническите познания, опитът, образованието и обучението, които се очакват от ползвателя, и средата, в която е предвидено да се използва системата.

5. Високорисковите системи с ИИ се изпитват с цел определяне на най-подходящите мерки за управление на риска. Изпитванията гарантират, че високорисковите системи с ИИ функционират стабилно с оглед на своето предназначение и са в съответствие с изискванията, определени в настоящата глава.
6. Изпитвателните процедури трябва да бъдат подходящи за постигане на предназначението на системата с ИИ и да не надхвърлят необходимото за постигането на тази цел.
7. Изпитването на високорисковите системи с ИИ се извършва, както е целесъобразно, във всеки момент от процеса на разработка и — при всички случаи — преди пускането на пазара или въвеждането в експлоатация. Изпитването се извършва спрямо предварително определени показатели и вероятностни прагове, които са подходящи с оглед на предназначението на високорисковата система с ИИ.
8. При прилагането на системата за управление на риска, описана в параграфи 1—7, специално се отчита дали е вероятно достъп до високорисковата система с ИИ да имат деца или тя да оказва въздействие върху тях.
9. За кредитни институции по Директива 2013/36/ЕС аспектите, описани в параграфи 1—8, представляват част от процедурите за управление на риска,

създавани от тези институции в съответствие с член 74 от посочената директива.

Член 10

Данни и управление на данните

1. Високорисковите системи с ИИ, при които се използват техники, предполагащи обучение на модели с данни, се разработват въз основа на набори от обучителни, валидационни и изпитвателни данни, които отговарят на критериите за качество, посочени в параграфи 2—5.
2. Наборите от обучителни, валидационни и изпитвателни данни трябва да бъдат обект на подходящи практики за управление и менажиране на данните. Тези практики се отнасят по-специално до:
 - а) съответните проектантски решения;
 - б) събирането на данни;
 - в) съответните операции по подготовка на данните, като аотиране, етикетиране, прочистване, обогатяване и агрегиране;
 - г) формулирането на съответните допускания, по-специално по отношение на информацията, която данните следва да измерват и представят;
 - д) предварителната оценка на наличието, качеството и устойчивостта на необходимите набори от данни;
 - е) преглед с оглед на евентуална предубеденост;
 - ж) идентифициране на евентуални недостатъци на данните, празноти в тях и на начини за тяхното отстраняване.
3. Наборите от обучителни, валидационни и изпитвателни данни трябва да бъдат подходящи, представителни и пълни и да не съдържат грешки. Те трябва да притежават подходящите статистически свойства, включително, където е приложимо, по отношение на лицата или групите лица, по отношение на които ще се използва високорисковата система с ИИ. Тези характеристики на наборите от данни могат да бъдат постигнати на равнището на отделните набори от данни или по отношение на комбинация от тях.
4. Наборите от обучителни, валидационни и изпитвателни данни отчитат — доколкото това е необходимо с оглед на предназначението — характеристиките или елементите, специфични за конкретните географски, поведенчески или функционални условия, в които е предвидено да се използва високорисковата система с ИИ.
5. Доколкото това е строго необходимо за целите на осигуряването на мониторинг, откриване и коригиране на предубедеността във високорисковите системи с ИИ, доставчиците на такива системи могат да обработват специални категории лични данни, посочени в член 9, параграф 1 от Регламент (ЕС) 2016/679, член 10 от Директива (ЕС) 2016/680 и член 10, параграф 1 от Регламент (ЕС) 2018/1725, като обезпечават подходящи гаранции за правата и свободите на физическите лица, включително технически ограничения относно повторното използване и използването на най-съвременни мерки за сигурност и опазване на личния живот, когато анонимизирането може да има значително отражение върху преследваната цел.

6. При разработката на високорискови системи с ИИ се прилагат подходящи практики за за мащабно или непосредствено управление на данните с изключение на системи, при които се използват техники, които предполагат обучаване на модели с цел да се гарантира, че тези високорискови системи с ИИ са в съответствие с параграф 2.

Член 11

Техническа документация

1. Техническата документация на една високорискова система с ИИ се изготвя преди тя да бъде пусната на пазара или въведена в експлоатация и се поддържа актуална.

Техническата документация се изготвя по такъв начин, че да показва, че високорисковата система с ИИ съответства на изискванията, определени в настоящата глава, и предоставя на националните компетентни органи и нотифицираните органи цялата необходима информация за оценяване на съответствието на системата с посочените изисквания. Тя съдържа най-малко елементите, определени в приложение IV.
2. Когато на пазара се пуска или в експлоатация се въвежда високорискова система с ИИ, свързана с продукт, към който се прилагат правните актове, посочени в приложение II, раздел А, се изготвя една-единствена техническа документация, съдържаща цялата информация, посочена в приложение IV, както и информацията, изисквана съгласно тези законодателни актове.
3. На Комисията се предоставя правомощието да приема делегирани актове в съответствие с член 73 за изменение на приложение IV, когато това е необходимо, за да се гарантира, че в светлината на техническия напредък, техническата документация предоставя всичката необходима информация за оценяване на съответствието на системата с изискванията, определени в настоящата глава.

Член 12

Поддържане на регистри

1. Високорисковите системи с ИИ се проектират и разработват с възможности за автоматично записване на събития („записи“) по време на работа на системата с ИИ. Тези възможности за създаване на записи трябва да отговарят на признати стандарти или общи спецификации.
2. Възможностите за създаване на записи трябва да гарантират равнище на проследимост на функционирането на системата с ИИ по време на нейния експлоатационен срок, което е подходящо с оглед на нейното предназначение.
3. По-специално възможностите за създаване на записи трябва да дават възможност за мониторинг на работата на високорисковата система с ИИ по отношение на настъпването на ситуации, които могат да доведат до това системата с ИИ да представлява риск по смисъла на член 65, параграф 1 или да доведат до съществено изменение, както и да улесняват мониторинга след пускането на пазара, посочен в член 61.
4. За високорисковите системи с ИИ, посочени в параграф 1, буква а) от приложение III, възможностите за запис трябва да осигуряват най-малкото:

- а) записване на периода на всяко използване на системата (начални дата и час и крайни дата и час на всяко използване);
- б) референтната база данни, спрямо която системата е проверявала входящите данни;
- в) входящите данни, за които търсенето е довело до съвпадение;
- г) идентификация на физическите лица, участвали във верификацията на резултатите, посочени в член 14, параграф 5.

Член 13

Прозрачност и предоставяне на информация на ползвателите

1. Високорисковите системи с ИИ се проектират и разработват по такъв начин, че да се гарантира, че тяхната работа е достатъчно прозрачна, за да могат ползвателите да тълкуват резултатите, получени от системата, и да ги използват по подходящ начин. Осигурява се подходящ вид и степен на прозрачност с оглед на постигане на съответствие с приложимите задължения на ползвателя и доставчика, посочени в глава 3 от настоящия дял.
2. Високорисковите системи с ИИ се придружават от инструкции за употреба в подходящ цифров или друг формат, които включват кратка, пълна, вярна и ясна информация, която е уместна, достъпна и разбираема за ползвателите.
3. В посочената в параграф 2 информация се посочват:
 - а) данните, които идентифицират доставчика и координатите за връзка с него и, когато е приложимо, тези на неговия упълномощен представител;
 - б) характеристиките, възможностите и ограниченията в действието на високорисковата система с ИИ, включително:
 - i) нейното предназначение;
 - ii) степента на точност, надеждност и киберсигурност, посочена в член 15, с оглед на която е изпитана и валидирана високорисковата система с ИИ, както и евентуални известни или предвидими обстоятелства, които могат да окажат въздействие върху очакваното ниво на точност, надеждност и киберсигурност;
 - iii) евентуални известни или предвидими обстоятелства, свързани с използването на високорисковата система с ИИ в съответствие с предназначението ѝ или в условия на разумно предвидима неправилна експлоатация, които могат да доведат до рискове за здравето и безопасността или за основните права;
 - iv) действието ѝ по отношение на лицата или групите лица, спрямо които системата е предназначена да се използва;
 - v) когато е целесъобразно, спецификации на входящите данни или всякаква друга относима информация по отношение на наборите от обучителни, валидационни и изпитвателни данни, като се отчита предназначението на системата с ИИ;
 - в) промените във високорисковата система с ИИ и в нейното действие, които са били предварително определени от доставчика към момента на първоначалното оценяване на съответствието, ако има такива;

- г) мерките за човешки надзор, посочени в член 14, включително техническите мерки, въведени с цел улесняване на тълкуването от страна на ползвателите на крайния резултат, получен от системите с ИИ;
- д) очакваният срок на експлоатация на високорисковата система с ИИ и евентуално необходимите мерки за поддръжка и обслужване с цел да се гарантира правилното функциониране на системата с ИИ, включително по отношение на актуализациите на софтуера.

Член 14
Човешки надзор

1. Високорисковите системи с ИИ се проектират и разработват — включително като се предвиждат подходящи инструменти за интерфейса човек—машина в тях — по такъв начин, че върху тях да може да бъде упражняван ефективен надзор от физически лица в периода, през който те се използват.
2. Човешкият надзор има за цел предотвратяването или свеждането до минимум на рисковете за здравето, безопасността или основните права, които могат да възникнат при използването на система с ИИ в съответствие с нейното предназначение или в условия на разумно предвидима неправилна експлоатация, по-специално когато тези рискове продължават да съществуват, независимо от прилагането на останалите изисквания, определени в настоящата глава.
3. Човешкият надзор се осигурява чрез една или всички от следните мерки:
 - а) мерки, които са идентифицирани и вградени, когато това е технически осъществимо, във високорисковата система с ИИ от доставчика преди пускането ѝ на пазара или въвеждането ѝ в експлоатация;
 - б) мерки, които са идентифицирани от доставчика преди пускането на високорисковата система с ИИ на пазара или въвеждането ѝ в експлоатация и които са подходящи за прилагане от страна на ползвателя.
4. Мерките, посочени в параграф 3, трябва да дават възможност на лицата, на които е възложено да упражняват човешки надзор, да извършват следните, както е уместно с оглед на обстоятелствата:
 - а) изцяло да разбират възможностите и ограниченията на високорисковата система с ИИ и да могат надлежно да следят нейното функциониране, така че признаците за аномалии, дисфункции и неочаквано действие да могат да бъдат откривани и спрямо тях да бъдат предприемани действия възможно най-бързо;
 - б) да си дават сметка за възможната тенденция автоматично да се разчита или в прекалено голяма степен да се разчита на резултатите, получени от високорискова система с ИИ („предубеденост в полза на автоматизираните решения“), по-специално за високорискови системи с ИИ, използвани за предоставяне на информация или препоръки във връзка с решения, които се вземат от физически лица;
 - в) да бъдат в състояние да тълкуват правилно резултатите от високорисковата система с ИИ, като вземат предвид по-специално характеристиките на системата и наличните инструменти и методи за тълкуване;

- г) да бъдат в състояние да вземат решение — във всяка една конкретна ситуация — да не използват резултата от високорисковата система с ИИ или по друг начин да го игнорират, потиснат или отменят;
 - д) да бъдат в състояние да се намесят в работата на високорисковата система с ИИ или да прекъснат системата чрез стоп бутон или подобна процедура.
5. За високорисковите системи с ИИ, посочени в точка 1, буква а) от приложение III, мерките, посочени в параграф 3, трябва да бъдат такива, че да гарантират в допълнение, че ползвателят не предприема действия, нито взема решения въз основа на идентификацията, посочена от системата, освен ако тя е била верифицирана и потвърдена от поне две физически лица.

Член 15

Точност, надеждност и киберсигурност

1. Високорисковите системи с ИИ се проектират и разработват така, че да постигат с оглед на предназначението си подходящо ниво на точност, надеждност и киберсигурност и да функционират стабилно в тези отношения в течение на експлоатационния си срок.
2. Нивата на точност и съответните показатели за точност на високорисковите системи с ИИ се обявяват в придружаващите я инструкции за употреба.
3. Високорисковите системи с ИИ трябва да бъдат устойчиви по отношение на грешки, недостатъци или несъответствия, евентуално възникващи в рамките на системата или на средата, в която тя работи, по-специално поради взаимодействието им с физически лица или други системи.

Надеждността на високорисковите системи с ИИ може да бъде постигната чрез решения за техническо дублиране, които могат да включват резервни или аварийни планове.

Високорисковите системи с ИИ, които продължават да се обучават след пускането им на пазара или въвеждането им в експлоатация, трябва да бъдат разработени така, че да се гарантира, че по отношение на евентуално опорочените от предубеденост резултати, дължащи се на използването на резултати като входящи данни за бъдещи операции („обратни връзки“), се вземат надлежно подходящите ограничителни мерки.

4. Високорисковите системи с ИИ трябва да бъдат устойчиви по отношение на опитите на неоправомощени трети страни да променят използването или действието им, като използват слабите места на системата.

Техническите решения, целящи да гарантират киберсигурността на високорисковите системи с ИИ, трябва да бъдат съобразени със съответните обстоятелства и рискове.

Техническите решения за преодоляване на специфичните за ИИ слаби места включват, където е целесъобразно, мерки за предотвратяване и контрол на атаки, целящи да манипулират набора от обучителни данни („отравяне на данните“), за предотвратяване на входящи данни, разработени с цел да накарат модела да допусне грешка („враждебни примери“), или на пороци на модела.

ГЛАВА 3

ЗАДЪЛЖЕНИЯ НА ДОСТАВЧИЦИТЕ И ПОЛЗВАТЕЛИТЕ НА ВИСОКОРИСКОВИ СИСТЕМИ С ИИ И НА ДРУГИ СТРАНИ

Член 16

Задължения на доставчиците на високорисковите системи с ИИ

Доставчиците на високорисковите системи с ИИ:

- а) гарантират, че техните системи с ИИ съответстват на изискванията, определени в глава 2 от настоящия дял;
- б) разполагат със система за управление на качеството, която е в съответствие с член 17;
- в) изготвят техническата документация на високорисковата система с ИИ;
- г) когато са под техен контрол, съхраняват записите, автоматично направени от техните високорисковите системи с ИИ;
- д) гарантират, че високорисковата система с ИИ преминава през съответната процедура за оценяване на съответствието, преди да бъде пусната на пазара или въведена в експлоатация;
- е) изпълняват регистрационните задължения, посочени в член 51;
- ж) предприемат необходимите корективни действия, ако високорисковата система с ИИ не е в съответствие с изискванията, определени в глава 2 от настоящия дял;
- з) уведомяват националните компетентни органи на държавите членки, в които са предоставили системата с ИИ на пазара или са я въвели в експлоатация и, където е приложимо, нотифицирания орган за несъответствието и за евентуалните предприети корективни действия;
- и) поставят маркировката „СЕ“ на своите високорисковите системи с ИИ, за да укажат съответствието с настоящия регламент съгласно член 49;
- й) по искане на национален компетентен орган доказват съответствието на високорисковата система с ИИ с изискванията, определени в глава 2 от настоящия дял.

Член 17

Система за управление на качеството

1. Доставчиците на високорисковите системи с ИИ въвеждат система за управление на качеството, която гарантира съответствие с настоящия регламент. Системата се документира системно и последователно чрез политики, процедури и инструкции в писмен вид и включва най-малко следните аспекти:
 - а) стратегия за регулаторно съответствие, включително съответствие с процедурите за оценяване на съответствието и процедурите за управление на модификациите на високорисковата система с ИИ;

- б) техники, процедури и системни действия, които да се използват при проектирането, проектния контрол и проектната верификация на високорисковата система с ИИ;
 - в) техники, процедури и системни действия, които да се използват за разработката, контрола на качеството и осигуряването на качеството на високорисковата система с ИИ;
 - г) процедури за проверка, изпитване и валидиране, които да се извършват преди, по време на и след разработването на високорисковата система с ИИ, и честотата, с която те трябва да се извършват;
 - д) технически спецификации, включително стандарти, които да се прилагат и, когато съответните хармонизирани стандарти не са приложени изцяло, средствата, които трябва да се използват, за да се гарантира, че високорисковата система с ИИ съответства на изискванията, определени в глава 2 от настоящия дял;
 - е) системи и процедури за управление на данни, включително събиране, анализ, етикетиране, съхранение, филтриране, извличане, агрегиране, запазване на данни, както и за всякакви други операции по отношение на данните, които се извършват преди и за целите на пускането на пазара или въвеждането в експлоатация на високорискови системи с ИИ;
 - ж) системата за управление на риска, посочена в член 9;
 - з) създаването, въвеждането и поддържането на система за мониторинг след пускане на пазара в съответствие с член 61;
 - и) процедури, свързани с докладването на сериозни инциденти и на повреди в съответствие с член 62;
 - й) придвижването на комуникацията с националните компетентни органи, компетентните органи, включително секторните, осигуряващи или съдействащи за достъпа до данни, нотифицираните органи, другите оператори, потребителите или други заинтересовани страни;
 - к) системи и процедури за поддържане на регистри на всичката имаща отношение документация и информация;
 - л) управление на ресурсите, включително мерки, свързани със сигурността на доставките;
 - м) рамка за отчетност, определяща отговорностите на ръководния състав и останалите служители по отношение на всички аспекти, посочени в настоящия параграф.
2. Реализацията на аспектите, посочени в параграф 1, е пропорционална на размера на организацията на доставчика.
3. За доставчици, които са кредитни институции, по отношение на които се прилага Директива 2013/36/ЕС, задължението за въвеждане на система за управление на качеството се счита за изпълнено чрез съответствието с правилата за вътрешното управление, процесите и механизмите съгласно член 74 от посочената директива. В този контекст се вземат предвид евентуалните хармонизирани стандарти, посочени в член 40 от настоящия регламент.

Член 18

Задължение за изготвяне на техническа документация

1. Доставчиците на високорискови системи с ИИ изготвят техническата документация, посочена в член 11, в съответствие с приложение IV.
2. Доставчиците, които са кредитни институции, по отношение на които се прилага Директива 2013/36/ЕС, поддържат техническата документация като част от документацията относно вътрешното управление, процесите и механизмите съгласно член 74 от посочената директива.

Член 19

Оценяване на съответствието

1. Доставчиците на високорискови системи с ИИ гарантират, че техните системи преминават през съответната процедура за оценяване на съответствието съгласно член 43, преди да бъдат пуснати на пазара или въведени в експлоатация. Когато съответствието на системите с ИИ с изискванията, определени в глава 2 от настоящия дял, бъде доказано след оценяването на съответствието, доставчиците изготвят декларация за съответствие с изискванията на ЕС съгласно член 48 и поставят маркировка за съответствие „СЕ“ съгласно член 49.
2. За високорисковите системи с ИИ, посочени в точка 5, буква б) от приложение III, пуснати на пазара или въведени в експлоатация от доставчици, които са кредитни институции, за които се прилага Директива 2013/36/ЕС, оценяването на съответствието се извършва като част от процедурата, посочена в членове 97—101 от същата директива.

Член 20

Автоматично генерирани записи

1. Доставчиците на високорискови системи с ИИ съхраняват записите, автоматично генерирани от техните високорискови системи с ИИ, доколкото тези записи са под техен контрол по силата на договорни взаимоотношения с ползвателя или по закон. Записите се съхраняват за срок, който е подходящ с оглед на предназначението на високорисковата система с ИИ и приложимите правни задължения съгласно правото на Съюза или националното право.
2. Доставчиците, които са кредитни институции, регулирани от Директива 2013/36/ЕС, поддържат записите, автоматично генерирани от техните високорискови системи с ИИ, като част от документацията по член 74 от посочената директива.

Член 21

Корективни действия

Доставчиците на високорискови системи с ИИ, които считат или имат основание да считат, че дадена високорискова система с ИИ, която са пуснали на пазара или въвели в експлоатация, не съответства на настоящия регламент, незабавно предприемат необходимите корективни действия, за да приведат системата в съответствие, да я изтеглят или да я изземат, както е необходимо. Те информират съответно дистрибуторите на въпросната високорискова система с ИИ и, ако е приложимо, упълномощения представител и вносителите.

Член 22
Задължение за информиране

Когато високорисковата система с ИИ представлява риск по смисъла на член 65, параграф 1 и този риск е известен на доставчика на системата, доставчикът незабавно уведомява националните компетентни органи на държавите членки, в които е предоставил системата и, където е приложимо, нотифицирания орган, издал сертификат за високорисковата система с ИИ, по-специално за несъответствието и за евентуалните предприети корективни действия.

Член 23
Сътрудничество с компетентните органи

При поискване от национален компетентен орган доставчиците на високорискови системи с ИИ предоставят на този орган цялата информация и документация, необходима за доказване на съответствието на високорисковата система с ИИ с изискванията, определени в глава 2 от настоящия дял, на официален език на Съюза, определен от съответната държава членка. При мотивирано искане от национален компетентен орган доставчиците също така дават на този орган достъп до записите, автоматично генерирани от високорисковата система с ИИ, доколкото тези записи са под техен контрол по силата на договорни взаимоотношения с ползвателя или по закон.

Член 24
Задължения на производителите на продукти

Когато високорискова система с ИИ, свързана с продукти, към които се прилагат законодателните актове, посочени в приложение II, раздел А, се пуска на пазара или се въвежда в експлоатация заедно с произведения продукт в съответствие с тези законодателни актове и с името на производителя на продукта, производителят на продукта носи отговорността за съответствието на системата с ИИ с настоящия регламент и, що се отнася до системата с ИИ, има същите задължения като наложените с настоящия регламент на доставчика.

Член 25
Упълномощени представители

1. Когато даден вносител не може да бъде идентифициран, преди да предоставят неговите системи на пазара на Съюза, доставчиците, установени извън Съюза, чрез писмено пълномощно определят упълномощен представител, който е установен в Съюза.
2. Упълномощеният представител изпълнява задачите, определени в пълномощното, получено от доставчика. Пълномощното дава право на упълномощения представител да извършва следните задачи:
 - а) да съхранява копие от декларацията за съответствие с изискванията на ЕС и от техническата документация, което да е на разположение на националните компетентни органи и националните органи, посочени в член 63, параграф 7;
 - б) при мотивирано искане да предоставя на националния компетентен орган всичката информация и документация, необходима за доказване на съответствието на дадена високорискова система с ИИ с изискванията, определени в глава 2 от настоящия дял, включително достъп до записите,

генерирани автоматично от високорисковата система с ИИ, доколкото тези записи са под контрола на доставчика по силата на договорни взаимоотношение с ползвателя или по закон;

- в) при мотивирано искане да си сътрудничи с компетентните национални органи в евентуалните действия, които те предприемат във връзка с високорисковата система с ИИ.

Член 26

Задължения на вносителите

1. Преди да пуснат на пазара високорискова система с ИИ вносителите на тази система гарантират, че:
 - а) съответната процедура за оценяване на съответствието е била проведена от доставчика на тази система с ИИ;
 - б) доставчикът е изготвил техническата документация в съответствие с приложение IV;
 - в) системата е означена с изискваната маркировка за съответствие и е придружена от изискваната документация и инструкции за употреба.
2. Когато вносител счита или има основание да счита, че дадена високорискова система с ИИ не е в съответствие с настоящия регламент, той не пуска тази система на пазара преди тя да бъде приведена в съответствие. Когато високорисковата система с ИИ представлява риск по смисъла на член 65, параграф 1, вносителят уведомява за това доставчика на системата с ИИ и органите за надзор на пазара.
3. Вносителите посочват своето име, регистрирано търговско наименование или регистрирана търговска марка и адреса, на който с тях може да бъде установен контакт, върху високорисковата система с ИИ, или, когато това не е възможно — върху нейната опаковка или придружаваща документация, както е приложимо.
4. Вносителите гарантират, че докато отговарят за една високорискова система с ИИ, условията на съхранение или транспортиране, когато такива са приложими, не застрашават съответствието ѝ с изискванията, определени в глава 2 от настоящия дял.
5. При мотивирано искане вносителите предоставят на националните компетентни органи всичката информация и документация, необходима за доказване на съответствието на дадена високорискова система с ИИ с изискванията, определени в глава 2 от настоящия дял, на език, който е лесно разбираем за съответния национален компетентен орган, включително достъп до записите, генерирани автоматично от високорисковата система с ИИ, доколкото тези записи са под контрола на доставчика по силата на договорни взаимоотношение с ползвателя или по закон. Те също така си сътрудничат и с посочените органи в евентуалните действия, които националният компетентен орган предприема във връзка с тази система.

Член 27

Задължения на дистрибуторите

1. Преди да предоставят високорискова система с ИИ на пазара, дистрибуторите се уверяват, че тя има нанесена изискваната маркировка за съответствие „СЕ“, че е придружена от необходимата документация и инструкции за употреба и че доставчикът и вносителят на системата, както е приложимо, са изпълнили задълженията, определени в настоящия регламент.
2. Когато дистрибутор счита или има основание да счита, че дадена високорискова система с ИИ не е в съответствие с изискванията, определени в глава 2 от настоящия дял, той не предоставя тази система на пазара преди тя да бъде приведена в съответствие с тези изисквания. Освен това, когато системата представлява риск по смисъла на член 65, параграф 1, дистрибуторът уведомява за това, както е приложимо, доставчика или вносителя на системата.
3. Дистрибуторите гарантират, че докато отговарят за една високорискова система с ИИ, условията на съхранение или транспортиране, когато такива са приложими, не застрашават съответствието на системата с изискванията, определени в глава 2 от настоящия дял.
4. Дистрибутор, който счита или има основание да счита, че дадена високорискова система с ИИ, която е предоставил на пазара, не е в съответствие с изискванията, определени в глава 2 от настоящия дял, предприема необходимите корективни действия за привеждането ѝ в съответствие с посочените изисквания, за изтеглянето или изземването ѝ или гарантира, че съответно доставчикът, вносителят или всеки имащ отношение оператор предприема посочените корективни действия. Когато високорисковата система с ИИ представлява риск по смисъла на член 65, параграф 1, дистрибуторът незабавно уведомява националните компетентни органи на държавите членки, в които е предоставил продукта, като предоставя подробни данни, по-специално за несъответствието и за евентуалните предприети корективни действия.
5. При мотивирано искане от национален компетентен орган дистрибуторите на високорискови системи с ИИ предоставят на този орган всичката информация и документация, необходима за доказване на съответствието на високорисковата система с изискванията, определени в глава 2 от настоящия дял. Дистрибуторите си сътрудничат също така с този национален компетентен орган в евентуалните действия, предприети от него.

Член 28

Задължения на дистрибуторите, вносителите, ползвателите и всички други трети страни

1. Всеки дистрибутор, вносител, ползвател или друга трета страна се счита за доставчик за целите на настоящия регламент и за обект на задълженията на доставчика съгласно член 16, в следните случаи:
 - а) той пуска на пазара или въвежда в експлоатация високорискова система с ИИ със своето име или търговска марка;
 - б) той изменя предназначението на високорискова система с ИИ, която вече е пусната на пазара или въведена в експлоатация;

- в) той прави значителни изменения във високорисковата система с ИИ.
2. При настъпване на обстоятелствата, посочени в параграф 1, буква б) или в), доставчикът, който първоначално е пуснал на пазара високорисковата система с ИИ или я е въвел в експлоатация, повече не се счита за доставчик за целите на настоящия регламент.

Член 29

Задължения на ползвателите на високорискови системи с ИИ

1. Ползвателите на високорискови системи с ИИ използват тези системи в съответствие с инструкциите за употреба, които ги придружават съгласно параграфи 2 и 5.
2. Задълженията съгласно параграф 1 не засягат други задължения на ползвателите съгласно правото на Съюза или националното право и свободата на преценка на ползвателя как да организира собствените си ресурси и дейности с цел изпълнение на мерките за човешки надзор, посочени от доставчика.
3. Без да се засяга параграф 1 и доколкото ползвателят упражнява контрол върху входящите данни, той гарантира, че тези входящи данни са подходящи с оглед на предназначението на високорисковата система с ИИ.
4. Ползвателите следят функционирането на високорисковата система с ИИ въз основа на инструкциите за употреба. Когато имат основания да считат, че използването в съответствие с инструкциите за употреба може да доведе до това системата с ИИ да представлява риск по смисъла на член 65, параграф 1, те уведомяват доставчика или дистрибутора и спират използването на системата. Те уведомяват доставчика или дистрибутора също при констатиране на сериозен инцидент или неизправност по смисъла на член 62 и прекъсват използването на системата с ИИ. В случай че ползвателят не може да се свърже с доставчика, член 62 се прилага *mutatis mutandis*.

За ползватели, които са кредитни институции, по отношение на които се прилага Директива 2013/36/ЕС, задължението за мониторинг, предвидено в първа алинея, се счита за изпълнено чрез съответствието с правилата за вътрешното управление, процесите и механизмите съгласно член 74 от посочената директива.

5. Ползвателите на високорискови системи с ИИ съхраняват записите, автоматично генерирани от техните високорискови системи с ИИ, доколкото тези записи са под техен контрол. Записите се съхраняват за срок, който е подходящ с оглед на предназначението на високорисковата система с ИИ и приложимите правни задължения съгласно правото на Съюза или националното право.

Ползвателите, които са кредитни институции, по отношение на които се прилага Директива 2013/36/ЕС, поддържат записите като част от документацията относно вътрешното управление, процесите и механизмите съгласно член 74 от посочената директива.

6. Ползвателите на високорискови системи с ИИ използват информацията, предоставена съгласно член 13, за да изпълняват задължението си за извършване на оценка на въздействието по отношение на защитата на данните

съгласно член 35 от Регламент (ЕС) 2016/679 или член 27 от Директива (ЕС) 2016/680, където е приложимо.

ГЛАВА 4

НОТИФИЦИРАЩИ ОРГАНИ И НОТИФИЦИРАНИ ОРГАНИ

Член 30

Нотифициращи органи

1. Всяка държава членка определя или създава нотифициращ орган, който отговаря за въвеждането и извършването на необходимите процедури за оценяването, определянето и нотифицирането на органи за оценяване на съответствието и за провеждането на мониторинг по отношение на тях.
2. Държавите членки могат да определят национален орган по акредитация, посочен в Регламент (ЕО) № 765/2008, като нотифициращ орган.
3. Нотифициращите органи се създават, организират и функционират по такъв начин, че да не възниква конфликт на интереси с органите за оценяване на съответствието и обективността и безпристрастността на техните действия да бъдат гарантирани.
4. Нотифициращите органи се организират по такъв начин, че решенията, свързани с нотифицирането на органи за оценяване на съответствието, се вземат от компетентни лица, различни от тези, които са извършили оценяването на тези органи.
5. Нотифициращите органи не могат да предлагат или извършват никоя от дейностите, които извършват органите за оценяване на съответствието, нито да предоставят консултантски услуги с търговска цел или на конкурентна основа.
6. Нотифициращите органи гарантират поверителността на информацията, която получават.
7. Нотифициращите органи разполагат с достатъчен брой компетентен персонал, необходим за правилното изпълнение на техните задачи.
8. Нотифициращите органи гарантират, че оценяването на съответствието се извършва по пропорционален начин, като се избягва ненужната тежест за доставчиците и че нотифицираните органи извършват дейностите си, като надлежно отчитат размера на даденото предприятие, сектора на дейност, структурата му и степента на сложност на въпросната система с ИИ.

Член 31

Заявление за нотифициране, което подава органът за оценяване на съответствието

1. Органите за оценяване на съответствието подават заявления за нотифициране до нотифициращия орган на държавата членка, в която са установени.
2. Заявлението за нотифициране се придружава от описание на дейностите по оценяване на съответствието, модул или модули за оценяване на съответствието и технологиите в сферата на изкуствения интелект, за които органът за оценяване на съответствието твърди, че е компетентен, както и от сертификат за акредитация, когато има такъв, издаден от национален орган по акредитация, който удостоверява, че органът за оценяване на съответствието

отговаря на изискванията, посочени в член 33. Добавят се и всякакви валидни документи, отнасящи се до съществуващи определения на подалия заявления нотифициран орган съгласно друго законодателство за хармонизация на Съюза.

3. Когато органът за оценяване на съответствието не може да представи сертификат за акредитация, той представя пред нотифициращия орган всички документи, необходими за проверката, признаването и редовното наблюдение на неговото съответствие с изискванията, посочени в член 33. За нотифицирани органи, които са определени съгласно друго законодателство за хармонизация на Съюза, всички документи и сертификати, свързани с тези определения, могат да се използват в подкрепа на процедурата за тяхното определяне съгласно настоящия регламент, както е целесъобразно.

Член 32

Процедура по нотифициране

1. Нотифициращите органи могат да нотифицират само органи за оценяване на съответствието, които отговарят на изискванията, определени в член 33.
2. Нотифициращите органи нотифицират Комисията и другите държави членки, като използват инструмента за електронно нотифициране, създаден и поддържан от Комисията.
3. Нотифицирането включва всички подробности за дейностите по оценяване на съответствието, модула или модулите за оценяване на съответствието и съответните технологии в сферата на изкуствения интелект.
4. Съответният орган за оценяване на съответствието може да изпълнява дейностите на нотифициран орган само ако в срок от един месец след нотифицирането не са направени възражения от Комисията или от другите държави членки.
5. Нотифициращите органи нотифицират Комисията и другите държави членки за всякакви последващи промени, свързани с нотификацията.

Член 33

Нотифицирани органи

1. Нотифицираните органи проверяват съответствието на високорисковите системи с ИИ с процедурите за оценяване на съответствието, посочени в член 43.
2. Нотифицираните органи отговарят на организационните изисквания, изискванията за управление на качеството, изискванията за ресурсите и процесите, необходими за изпълнението на техните задачи.
3. Организационната структура, разпределението на отговорностите, йерархичната структура и функционирането на нотифицираните органи трябва да бъдат такива, че да се гарантира доверието в провеждането от страна на нотифицираните органи и в резултатите от дейностите по оценяване на съответствието, които нотифицираните органи извършват.
4. Нотифицираните органи са независими от доставчика на дадена високорискова система с ИИ, по отношение на която извършват дейности по оценяване на съответствието. Нотифицираните органи са независими също така от всеки

друг оператор, който има икономически интерес от високорисковата система с ИИ, която се оценява, както и от евентуални конкуренти на доставчика.

5. Нотифицираните органи се организират и функционират така, че да се гарантират обективността и безпристрастността на техните дейности. Нотифицираните органи документират и въвеждат структура и процедури за гарантиране на безпристрастност и за насърчаване и прилагане на принципите на безпристрастност в цялата си организация, сред целия си персонал и в дейностите си по оценяване.
6. Нотифицираните органи имат документирани процедури, които гарантират, че техният персонал, комитети, подразделения, подизпълнители или друг свързан орган или персонал на външни органи спазват поверителността на информацията, получена при изпълнението на дейностите по оценяване на съответствието, освен когато нейното разгласяване се изисква по закон. Персоналът на нотифицираните органи е длъжен да пази служебна тайна по отношение на информацията, получена при изпълнение на задачите по настоящия регламент, освен по отношение на нотифициращите органи на държавата членка, в която осъществява дейността си.
7. Нотифицираните органи разполагат с процедури за изпълнение на дейностите си, които надлежно отчитат размера на дадено предприятие, сектора на дейност, неговата структура и степента на сложност на въпросната система с ИИ.
8. Нотифицираните органи сключват подходяща застраховка за покриване на отговорността си във връзка с дейностите си по оценяване на съответствието, освен когато отговорността се поема от съответната държава членка съгласно националното право или когато тази държава членка е пряко отговорна за оценяването на съответствието.
9. Нотифицираните органи трябва да могат да изпълняват всички задачи, възложени им съгласно настоящия регламент, с най-висока степен на почтено професионално поведение и необходимата компетентност в определената област, независимо дали тези задачи се изпълняват от самите нотифицирани органи или от тяхно име и на тяхна отговорност.
10. Нотифицираните органи разполагат с достатъчна собствена компетентност, за да могат ефективно да оценяват задачите, изпълнявани от външни страни от тяхно име. За целта по всяко време и за всяка процедура по оценяване на съответствието и за всеки тип високорискова система с ИИ, за които са определени, нотифицираните органи трябва да разполагат постоянно с достатъчен административен, технически и научен персонал с опит и знания в областта на съответните технологии в сферата на изкуствения интелект, данните и обработката на данни и по отношение на изискванията, определени в глава 2 от настоящия дял.
11. Нотифицираните органи участват в координационни дейности, както е предвидено в член 38. Те също така участват пряко или са представени в европейски организации за стандартизация или гарантират, че са запознати със съответните стандарти и актуалното им състояние.
12. Нотифицираните органи съхраняват на разположение на нотифициращия орган, посочен в член 30, и при поискване му предоставят цялата необходима документация, включително документацията на доставчика, за да осигурят на

този орган възможността да извършва дейностите си по оценяване, определяне, нотифициране, наблюдение и надзор и да улеснят оценяването, описано в настоящата глава.

Член 34

Поделения и възлагане на подизпълнители от страна на нотифицираните органи

1. В случаите, в които нотифициран орган възлага конкретни задачи, свързани с оценяване на съответствието, на подизпълнители или използва подразделенията си, той гарантира, че подизпълнителят или поделението отговаря на изискванията, определени в член 33, и информира нотифициращия орган за това.
2. Нотифицираните органи поемат пълната отговорност за задачите, изпълнявани от подизпълнители или подразделения, без значение къде са установени те.
3. Дейностите могат да бъдат възлагани на подизпълнители или изпълнявани от подразделения само със съгласието на доставчика.
4. Нотифицираните органи съхраняват на разположение на нотифициращия орган съответните документи относно оценката на квалификацията на подизпълнителя или на поделението и работата, извършена от тях съгласно настоящия регламент.

Член 35

Идентификационни номера и списъци на нотифицираните органи, определени съгласно настоящия регламент

1. Комисията определя идентификационен номер за всеки нотифициран орган. Тя определя само един-единствен номер дори когато органът е нотифициран съгласно няколко акта на Съюза.
2. Комисията прави обществено достояние списъка на нотифицираните съгласно настоящия регламент органи, включително определените им идентификационни номера и дейностите, за които те са били нотифицирани. Комисията поддържа този списък актуален.

Член 36

Промени в нотификациите

1. Когато нотифициращ орган подозира или е бил информиран, че нотифициран орган вече не отговаря на изискванията, определени в член 33, или че не изпълнява задълженията си, нотифициращият орган незабавно проучва въпроса възможно най-задълбочено. В тази връзка той уведомява съответния нотифициран орган за повдигнатите възражения и му дава възможност да изрази становището си. Ако нотифициращият орган стигне до заключението, че нотифицираният орган, обект на проучването, вече не отговаря на изискванията, определени в член 33, или че не изпълнява задълженията си, нотифициращият орган ограничава обхвата, спира действието или отменя нотификацията според случая, в зависимост от това колко съществени са пропуските. Той също така незабавно информира за това Комисията и другите държави членки.
2. В случай на ограничаване на обхвата, спиране на действието или оттегляне на нотификацията или в случай, че нотифицираният орган преустанови дейността

си, нотифициращият орган предприема подходящи стъпки, за да гарантира, че досиетата на този нотифициран орган се поемат от друг нотифициран орган или се съхраняват на разположение на отговорните нотифициращи органи при искане от тяхна страна.

Член 37

Оспорване на компетентността на нотифицирани органи

1. Когато това е необходимо, Комисията проучва всички случаи, при които има основания да се подозира съответствието на даден нотифициран орган с изискванията, определени в член 33.
2. Нотифициращият орган предоставя на Комисията, при искане от нейна страна, всичката информация, имаща отношение към нотификацията на съответния нотифициран орган.
3. Комисията гарантира, че всичката поверителна информация, получена в хода на проучването съгласно настоящия член, се третира като такава.
4. Когато Комисията констатира, че нотифициран орган не отговаря или вече не отговаря на изискванията, определени в член 33, тя приема мотивирано решение, с което от нотифициращата държава членка се изисква да предприеме необходимите корективни мерки, включително, ако е необходимо, оттегляне на нотификацията. Този акт за изпълнение се приема в съответствие с процедурата по разглеждане, посочена в член 74, параграф 2.

Член 38

Координация на нотифицираните органи

1. Комисията гарантира, че по отношение на областите, обхванати от настоящия регламент, между нотифицираните органи, работещи по процедури за оценяване на съответствието на системи с ИИ съгласно настоящия регламент, съществуват подходяща координация и подходящо сътрудничество и те правилно се провеждат под формата на секторна група от нотифицирани органи.
2. Държавите членки гарантират, че нотифицираните от тях органи участват в работата на тази група, пряко или чрез свои представители.

Член 39

Организации за оценяване на съответствието от трети държави

Организациите за оценяване на съответствието, учредени съгласно правото на трета държава, с която Съюзът е сключил споразумение, могат да бъдат оправомощени да извършват дейностите на нотифицираните органи съгласно настоящия регламент.

ГЛАВА 5

СТАНДАРТИ, ОЦЕНЯВАНЕ НА СЪОТВЕТСТВИЕТО, СРЕТИФИКАТИ, РЕГИСТРАЦИЯ

Член 40

Хармонизирани стандарти

Счита се, че високорисковите системи с ИИ, които съответстват на хармонизирани стандарти, данните за които са били публикувани в Официален вестник на Европейския съюз, или на части от тях, съответстват на посочените в глава 2 от настоящия дял изисквания, доколкото те са обхванати от тези стандарти.

Член 41

Общи спецификации

1. Когато не съществуват хармонизирани стандарти, като посочените в член 40, или когато Комисията прецени, че съответните хармонизирани стандарти са недостатъчни или че е необходимо да бъдат разгледани конкретни въпроси, които поражда опасения във връзка с безопасността или основните права, чрез актове за изпълнение Комисията може да приема общи спецификации по отношение на изискванията, установени в глава 2 от настоящия дял. Тези актове за изпълнение се приемат в съответствие с процедурата по разглеждане, посочена в член 74, параграф 2.
2. При изготвянето на общите спецификации, посочени в параграф 1, Комисията събира становищата на съответните органи или експертни групи, създадени съгласно приложимото секторно право на Съюза.
3. Високорисковите системи с ИИ, които отговарят на общите спецификации, посочени в параграф 1, се считат за съответстващи на изискванията, определени в глава 2 от настоящия дял, доколкото тези общи спецификации обхващат посочените изисквания.
4. Когато доставчиците не спазват общите спецификации, посочени в параграф 1, те надлежно доказват, че са приели технически решения, които са най-малко еквивалентни на тях.

Член 42

Презумпция за съответствие с определени изисквания

1. Като се има предвид тяхното предназначение, се приема, че високорисковите системи с ИИ отговарят на изискването по член 10, параграф 4, когато са били обучени и изпитани въз основа на данни, свързани със специфичните географски, поведенчески или функционални условия, в които е предвидено те да бъдат използвани.
2. Високорисковите системи с ИИ, които са сертифицирани или за които е издадена декларация за съответствие по схема за сертифициране на киберсигурността съгласно Регламент (ЕС) 2019/881 на Европейския

парламент и на Съвета⁶³ и чиито данни са били публикувани в *Официален вестник на Европейския съюз*, се считат за съответстващи на изискванията за киберсигурност, посочени в член 15 от настоящия регламент, доколкото сертификатът за киберсигурност или декларацията за съответствие или части от тях обхващат тези изисквания.

Член 43

Оценяване на съответствието

1. За високорисковите системи с ИИ, изброени в точка 1 от приложение III, когато при доказване на съответствието на високорискова система с ИИ с изискванията, определени в глава 2 от настоящия дял, доставчикът е приложил хармонизираните стандарти, посочени в член 40, или, когато е приложимо, общите спецификации, посочени в член 41, доставчикът следва една от изброените по-долу процедури:
 - а) процедурата за оценяване на съответствието въз основа на вътрешен контрол, посочена в приложение VI;
 - б) процедурата за оценяване на съответствието въз основа на система за управление на качеството и оценка на техническата документация с участието на нотифициран орган, посочена в приложение VII.

Когато при доказването на съответствието на високорискова система с ИИ с изискванията, определени в глава 2 от настоящия дял, доставчикът не е приложил или е приложил само частично хармонизираните стандарти, посочени в член 40, или когато такива хармонизирани стандарти не съществуват и липсват общи спецификации, като посочените в член 41, доставчикът следва процедурата за оценяване на съответствието, посочена в приложение VII.

За целите на процедурата за оценяване на съответствието, посочена в приложение VII, доставчикът може да избере всеки от нотифицираните органи. Когато обаче системата е предназначена за въвеждане в експлоатация от правоприлагащи органи, имиграционни органи или органи в областта на убежището, както и от институции, органи или агенции на ЕС, органът за надзор на пазара, посочен в член 63, параграф 5 или 6, според случая, действа като нотифициран орган.

2. За високорисковите системи с ИИ, посочени в точки 2—8 от приложение III, доставчиците следват процедурата за оценяване на съответствието въз основа на вътрешен контрол, посочена в приложение VI, която не предвижда участието на нотифициран орган. За високорисковите системи с ИИ, посочени в точка 5, буква б) от приложение III, пуснати на пазара или въведени в експлоатация от кредитни институции, регулирани от Директива 2013/36/ЕС, оценяването на съответствието се извършва като част от процедурата, посочена в членове 97—101 от същата директива.

⁶³ Регламент (ЕС) 2019/881 на Европейския парламент и на Съвета от 17 април 2019 г. относно ENISA (Агенцията на Европейския съюз за киберсигурност) и сертифицирането на киберсигурността на информационните и комуникационните технологии, както и за отмяна на Регламент (ЕС) № 526/2013 (Акт за киберсигурността) (ОВ L 151, 7.6.2019 г., стр. 1).

3. За високорисковите системи с ИИ, за които се прилагат правните актове, изброени в приложение II, раздел А, доставчикът следва съответното оценяване на съответствието, което се изисква съгласно тези правни актове. Изискванията, определени в глава 2 от настоящия дял, се прилагат за тези високорискови системи с ИИ и са част от това оценяване. Прилагат се също точки 4.3, 4.4 и 4.5, както и точка 4.6, пета алинея от приложение VII.

За целите на това оценяване нотифицираните органи, които са били нотифицирани съгласно тези правни актове, имат право да контролират дали високорисковите системи с ИИ отговарят на изискванията по глава 2 от настоящия дял, при условие че тези нотифицирани органи са спазили изискванията, предвидени в член 33, параграфи 4, 9 и 10, и това е било оценено в контекста на процедурата по нотифициране съгласно посочените правни актове.

Когато правните актове, изброени в приложение II, раздел А, дават възможност на производителя на продукта да се откаже от оценяване на съответствието като трета страна, при условие че този производител е приложил всички хармонизирани стандарти, обхващащи всички съответни изисквания, той може да използва тази възможност само ако е приложил и хармонизираните стандарти или, когато е приложимо, общите спецификации, посочени в член 41, обхващащи изискванията по глава 2 от настоящия дял.

4. Високорисковите системи с ИИ се подлагат на нова процедура за оценяване на съответствието, когато са съществено изменени, независимо дали изменената система е предназначена за по-нататъшно разпространение или продължава да се използва от настоящия ползвател.

За високорисковите системи с ИИ, които продължават да се обучават след пускането им на пазара или въвеждането им в експлоатация, промените във високорисковата система с ИИ и нейните показатели, които са били предварително определени от доставчика към момента на първоначалното оценяване на съответствието и са част от информацията, съдържаща се в техническата документация, посочена в точка 2, буква е) от приложение IV, не представляват съществено изменение.

5. На Комисията се предоставя правомощието да приема делегирани актове в съответствие с член 73 с цел актуализиране на приложения VI и VII, за да въвежда елементи на процедурите за оценяване на съответствието, които са станали необходими с оглед на техническия прогрес.
6. На Комисията се предоставя правомощието да приема делегирани актове за изменение на параграфи 1 и 2 с цел подлагане на високорисковите системи с ИИ, посочени в точки 2—8 от приложение III, на процедурата за оценяване на съответствието, посочена в приложение VII, или на части от нея. Комисията приема такива делегирани актове, като взема предвид ефективността на процедурата за оценяване на съответствието въз основа на вътрешен контрол, посочена в приложение VI, за предотвратяване или свеждане до минимум на рисковете за здравето и безопасността и защитата на основните права, породени от такива системи, както и наличието на подходящ капацитет и ресурси сред нотифицираните органи.

Член 44
Сертификати

1. Сертификатите, издадени от нотифицирани органи съгласно приложение VII, се изготвят на официален език на Съюза, определен от държавата членка, в която е установен нотифицираният орган, или на официален език на Съюза, приемлив за нотифицирания орган.
2. Сертификатите са валидни за указания в тях срок, като той не надхвърля пет години. По искане на доставчика валидността на сертификата може да се удължи за допълнителни срокове, всеки от които не надхвърля пет години, въз основа на последващо оценяване съгласно приложимите процедури за оценяване на съответствието.
3. Когато нотифициран орган установи, че система с ИИ е престанала да отговаря на изискванията по глава 2 от настоящия дял, въз основа на принципа на пропорционалност той спира действието или отнема издадения сертификат или налага ограничения върху него, освен когато съответствието с тези изисквания се осигури чрез подходящо коригиращо действие, което доставчикът на системата предприема в рамките на подходящ срок, определен от нотифицирания орган. Нотифицираният орган обосновава решението си.

Член 45
Обжалване на решения на нотифицираните органи

Държавите членки гарантират, че страните, които имат законен интерес от решенията на нотифицираните органи, разполагат с процедура за обжалване на тези решения.

Член 46
Задължения на нотифицираните органи за информиране

1. Нотифицираните органи информират нотифициращия орган за следното:
 - а) всички сертификати на Съюза за оценка на техническата документация, всички допълнения към тези сертификати, одобрения на системи за управление на качеството, издадени в съответствие с изискванията на приложение VII;
 - б) всеки отказ, ограничаване, спиране на действието или отнемане на сертификат на Съюза за оценка на техническата документация или одобрение на система за управление на качеството, издадени в съответствие с изискванията на приложение VII;
 - в) всякакви обстоятелства, които влияят върху обхвата или условията за нотифициране;
 - г) всякакви искания за информация, получени от органите за надзор на пазара, във връзка с дейности по оценяване на съответствието;
 - д) при поискване — за дейностите по оценяване на съответствието, извършени в обхвата на тяхната нотификация, и всякакви други извършени дейности, включително трансгранични, и дейности по възлагане на подизпълнители.
2. Всеки нотифициран орган информира останалите нотифицирани органи за:

- а) одобрения на системи за управление на качеството, които е отказал, спрял е действието им или е отнел, и при поискване — за издадените одобрения на системи за качество;
 - б) сертификати на ЕС за оценка на техническата документация или допълнения към тях, които е отказал, отнел, спрял е действието им или по друг начин е ограничил и, при поискване, на сертификатите и/или допълненията към тях, които е издал.
3. Всеки нотифициран орган предоставя на другите нотифицирани органи, осъществяващи подобни дейности по оценяване на съответствието, чийто предмет са същите технологии за изкуствен интелект, съответна информация по въпроси, свързани с отрицателни и, при поискване, положителни резултати от оценяването на съответствието.

Член 47

Дерогация от процедурата за оценяване на съответствието

1. Чрез дерогация от член 43 всеки орган за надзор на пазара може да разреши пускането на пазара или въвеждането в експлоатация на конкретни високорискови системи с ИИ на територията на съответната държава членка по изключителни причини, свързани с обществената сигурност или защитата на живота и здравето на хората, опазването на околната среда и защитата на ключови промишлени и инфраструктурни активи. Това разрешение се издава за ограничен период от време, докато се провеждат необходимите процедури за оценяване на съответствието, и се прекратява след приключването на тези процедури. Изпълнението на тези процедури се предприема без ненужно забавяне.
2. Разрешението, посочено в параграф 1, се издава само ако органът за надзор на пазара заключи, че високорисковата система с ИИ съответства на изискванията по глава 2 от настоящия дял. Органът за надзор на пазара информира Комисията и другите държави членки за всяко разрешение, издадено съгласно параграф 1.
3. Когато в рамките на 15 календарни дни от получаването на информацията, посочена в параграф 2, не е повдигнато възражение нито от държава членка, нито от Комисията във връзка с разрешение, издадено от орган за надзор на пазара на държава членка в съответствие с параграф 1, това разрешение се счита за обосновано.
4. Когато в срок от 15 календарни дни от получаването на нотификацията, посочена в параграф 2, държава членка повдигне възражения срещу разрешение, издадено от орган за надзор на пазара на друга държава членка, или когато Комисията прецени, че разрешението противоречи на правото на Съюза или че заключението на държавите членки относно съответствието на системата, посочено в параграф 2, е необосновано, Комисията незабавно започва консултации със съответната държава членка; провеждат се консултации със съответния(те) оператор(и) и му(им) се предоставя възможност да представи(ят) своето мнение. След като разгледа въпросното мнение Комисията решава дали разрешението е обосновано или не. Комисията адресира решението си до съответната държава членка и съответния оператор или оператори.

5. Ако се прецени, че разрешението не е обосновано, органът за надзор на пазара на съответната държава членка го оттегля.
6. Чрез дерогация от параграфи 1—5 за високорисковите системи с ИИ, предназначени да бъдат използвани като защитни елементи на устройства или които сами по себе си са устройства, попадащи в обхвата на Регламент (ЕС) 2017/745 и Регламент (ЕС) 2017/746, се прилагат член 59 от Регламент (ЕС) 2017/745 и член 54 от Регламент (ЕС) 2017/746 и по отношение на дерогацията от оценяването на съответствието с изискванията по глава 2 от настоящия дял.

Член 48

Декларация за съответствие с изискванията на ЕС

1. Доставчикът съставя писмена декларация за съответствие с изискванията на ЕС за всяка система с ИИ и я съхранява на разположение на националните компетентни органи в продължение на 10 години, след като системата с ИИ е била пусната на пазара или въведена в експлоатация. В декларацията за съответствие с изискванията на ЕС се посочва системата с ИИ, за която тя е изготвена. При поискване, на съответния национален компетентен орган се предоставя копие от декларацията за съответствие с изискванията на ЕС.
2. В нея се посочва, че въпросната високорискова система с ИИ отговаря на изискванията по глава 2 от настоящия дял. Декларацията за съответствие с изискванията на ЕС съдържа информацията, посочена в приложение V, и се превежда на официален(ни) език(ци) на Съюза, изискван(и) от държавата(ите) членка(и), в която(които) се предоставя високорисковата система с ИИ.
3. Когато високорисковите системи с ИИ са предмет на друго законодателство на Съюза за хармонизация, което също изисква декларация за съответствие с изискванията на ЕС, се изготвя единна декларация за съответствие с изискванията на ЕС по отношение на всички законодателни актове на Съюза, приложими към високорисковата система с ИИ. Декларацията съдържа цялата информация, необходима за установяване на законодателния акт на Съюза за хармонизация, с който е свързана съответната декларация.
4. Като изготвя декларацията за съответствие с изискванията на ЕС, доставчикът поема отговорността за съответствието с изискванията по глава 2 от настоящия дял. Доставчикът актуализира декларацията за съответствие с изискванията на ЕС, когато това е целесъобразно.
5. На Комисията се предоставя правомощието да приема делегирани актове в съответствие с член 73 за изменение на минималното съдържание на декларацията за съответствие с изискванията на ЕС по приложение V, за да се въведат елементи, които са станали необходими с оглед на техническия прогрес.

Член 49

Маркировка за съответствие „СЕ“

1. Маркировката „СЕ“ се нанася върху системите с ИИ по такъв начин, че да бъде видима, четлива и незаличима. Когато това не е възможно или не може да бъде гарантирано поради естеството на високорисковата система с ИИ, тя се полага върху опаковката или в придружаващите документи по целесъобразност.

2. Към маркировката „СЕ“, посочена в параграф 1 от настоящия член се прилагат общите принципи, определени в член 30 от Регламент (ЕО) № 765/2008.
3. Когато е приложимо, маркировката „СЕ“ е следвана от идентификационния номер на нотифицирания орган, отговарящ за процедурите за оценяване на съответствието по член 43. Идентификационният номер също се посочва върху всеки рекламен материал, който указва, че високорисковата система с ИИ отговаря на изискванията за маркировката „СЕ“.

Член 50

Съхранение на документи

В продължение на 10 години след пускането на пазара или въвеждането в експлоатация на системата с ИИ доставчикът съхранява на разположение на националните компетентни органи:

- а) техническата документация по член 11;
- б) документацията, свързана със системата за управление на качеството по член 17;
- в) когато е приложимо, документацията относно промените, одобрени от нотифицираните органи;
- г) когато е приложимо, решенията и другите документи, издадени от нотифицираните органи;
- д) декларацията за съответствие с изискванията на ЕС, посочена в член 48.

Член 51

Регистрация

Преди пускането на пазара или въвеждането в експлоатация на високорискова система с ИИ, посочена в член 6, параграф 2, доставчикът или, когато е приложимо, упълномощеният представител регистрира тази система в базата данни на ЕС, посочена в член 60.

ДЯЛ IV

ЗАДЪЛЖЕНИЯ ЗА ПРОЗРАЧНОСТ ЗА НЯКОИ СИСТЕМИ С ИИ

Член 52

Задължения за прозрачност за някои системи с ИИ

1. Доставчиците гарантират, че системите с ИИ, предназначени да взаимодействат с физически лица, са проектирани и разработени по такъв начин, че физическите лица да бъдат информирани, че взаимодействат със система с ИИ, освен ако това не е очевидно от обстоятелствата и контекста на употреба. Това задължение не се прилага за системи с ИИ, оправомощени по закон за разкриване, предотвратяване, разследване и наказателно преследване на престъпления, освен ако тези системи са на разположение на обществеността за съобщаване на престъпление.
2. Ползвателите на система за разпознаване на емоции или на система за биометрична категоризация информират физическите лица, които са обект на

нейното действие. Това задължение не се прилага за системи с ИИ, използвани за биометрична категоризация, които са разрешени от закона за разкриване, предотвратяване и разследване на престъпления.

3. Ползвателите на система с ИИ за генериране или обработка на изображения, аудио или видео съдържание, които до голяма степен наподобяват съществуващи лица, обекти, места или други субекти или събития и навярно някой би приел за автентични или достоверни („дълбинен фалшификат“), са задължени да разкрият, че съдържанието е било изкуствено създадено или обработено.

Първа алинея обаче не се прилага, когато използването е разрешено от закона за разкриване, предотвратяване, разследване и наказателно преследване на престъпления или е необходимо за упражняване на правото на свобода на изразяване на мнение и правото на свобода на изкуствата и науките, гарантирани от Хартата на основните права на ЕС, и при спазване на подходящи гаранции за правата и свободите на трети страни.

4. Параграфи 1, 2 и 3 не засягат изискванията и задълженията, установени в дял III от настоящия регламент.

Дял V

МЕРКИ В ПОДКРЕПА НА ИНОВАЦИИТЕ

Член 53

Регулаторни лаборатории в областта на ИИ

1. Регулаторните лаборатории в областта на ИИ, създадени от компетентните органи на една или повече държави членки или от Европейския надзорен орган по защита на данните, осигуряват контролирана среда, която улеснява разработването, изпитването и признаването на иновативни системи с ИИ за ограничен период от време преди пускането им на пазара или въвеждането им в експлоатация съгласно конкретен план. Това се извършва под прекия надзор и ръководство на компетентните органи, за да се гарантира спазването на изискванията на настоящия регламент и, когато е приложимо, на други законодателни актове на Съюза и на държавите членки, чието спазване е обект на надзор в рамките на регулаторната лаборатория.
2. Държавите членки гарантират, че доколкото иновативните системи с ИИ включват обработване на лични данни или по друг начин попадат в обхвата на надзорните правомощия на други национални органи или компетентни органи, предоставящи или подкрепящи достъпа до данни, националните органи за защита на данните и посочените други национални органи са свързани с функционирането на регулаторната лаборатория в областта на ИИ.
3. Регулаторните лаборатории в областта на ИИ не засягат надзорните и корективните правомощия на компетентните органи. Всички значителни рискове за здравето и безопасността и за основните права, установени по време на разработването и изпитването на такива системи, водят до незабавни ограничителни мерки, а при липса на такива – до спиране на процеса на разработване и изпитване до настъпването на въвеждане на въпросните мерки.

4. Участниците в регулаторната лаборатория в областта на ИИ продължават да носят отговорност съгласно приложимото законодателство на Съюза и на държавите членки за всяка вреда, причинена на трети страни в резултат на експериментирането, провеждано в регулаторна лаборатория.
5. Компетентните органи на държавите членки, които са създали регулаторни лаборатории в областта на ИИ, координират своите дейности и си сътрудничат в рамките на Европейския съвет по изкуствен интелект. Те представят на Съвета по ИИ и на Комисията годишни доклади относно резултатите от прилагането на тези схеми, включително добрите практики, извлечените поуки и препоръките относно тяхното създаване и, когато е приложимо, относно прилагането на настоящия регламент и на други законодателни актове на Съюза, които са обект на надзор в рамките на регулаторната лаборатория.
6. Условиата и редът за функциониране на регулаторните лаборатории в областта на ИИ, включително критериите за допустимост и процедурата за кандидатстване, подбор, участие и излизане от регулаторните лаборатории, както и правата и задълженията на участниците, се определят в актове за изпълнение. Тези актове за изпълнение се приемат в съответствие с процедурата по разглеждане, посочена в член 74, параграф 2.

Член 54

Последващо обработване на лични данни за разработване на някои системи с ИИ в обществен интерес в регулаторната лаборатория в областта на ИИ

1. В регулаторната лаборатория в областта на ИИ личните данни, събрани законно за други цели, се обработват за целите на разработването и изпитването на някои иновативни системи с ИИ при следните условия:
 - а) иновативните системи с ИИ се разработват за защита на значителен обществен интерес в една или повече от следните области:
 - i) предотвратяването, разследването, разкриването или наказателното преследване на престъпления или изпълнението на наложените наказания, включително предпазването от и предотвратяването на заплахи за обществената сигурност, под контрола и отговорността на компетентните органи. Обработването се основава на правото на държава членка или на Съюза;
 - ii) обществената безопасност и общественото здраве, включително профилактиката, контрола и лечението на болести;
 - iii) високо равнище на опазване и подобряване на качеството на околната среда;
 - б) обработваните данни са необходими за спазването на едно или повече от изискванията, посочени в дял III, глава 2, когато тези изисквания не могат да бъдат ефективно изпълнени чрез обработването на анонимизирани, синтетични или други нелични данни;
 - в) съществуват ефективни механизми за наблюдение, за да се установи дали могат да възникнат високи рискове за основните права на субектите на данни по време на експериментирането в регулаторната лаборатория, както и механизъм за реагиране с цел бързо ограничаване на тези рискове и, когато е необходимо, прекратяване на обработването;

- г) всички лични данни, които трябва да бъдат обработвани в рамките на регулаторната лаборатория, са във функционално отделна, изолирана и защитена среда за обработка на данни под контрола на участниците и само упълномощени лица имат достъп до тези данни;
 - д) обработваните лични данни не се предоставят или предават, нито други страни получават достъп до тях по друг начин;
 - е) никаква обработка на лични данни в контекста на регулаторната лаборатория не води до мерки или решения, засягащи субектите на данни;
 - ж) всички лични данни, обработвани в контекста на регулаторната лаборатория, се заличават, след като участието в нея завърши или личните данни достигнат края на срока си на съхранение;
 - з) записите за обработването на лични данни в контекста на регулаторната лаборатория се съхраняват за срока на участие в нея и 1 година след прекратяването на участието само докато е необходимо и единствено с оглед на изпълнението на задълженията за отчетност и документиране съгласно настоящия член или прилагането на друго законодателство на Съюза или на държавите членки;
 - и) пълното и подробно описание на процеса и обосновката за обучаването, изпитването и признаването на системата с ИИ се съхраняват заедно с резултатите от изпитванията като част от техническата документация в приложение IV;
 - й) кратко резюме на проекта за ИИ, разработен в регулаторната лаборатория, неговите цели и очаквани резултати, публикувани на уебсайта на компетентните органи.
2. Параграф 1 не засяга законодателството на Съюза или на държавите членки, изключващо обработването за цели, различни от изрично посочените в това законодателство.

Член 55

Мерки по отношение на малките доставчици и ползватели

1. Държавите членки предприемат следните действия:
- а) осигуряват на малките доставчици и стартиращите предприятия приоритетен достъп до регулаторните лаборатории в областта на ИИ, доколкото те отговарят на условията за участие;
 - б) организират специфични дейности за повишаване на осведомеността относно прилагането на настоящия регламент, съобразени с нуждите на малките доставчици и ползватели;
 - в) когато е целесъобразно, създават специален канал за комуникация с малки доставчици и ползватели и други новатори, за да предоставят насоки и да отговарят на запитванията относно прилагането на настоящия регламент.
2. При определянето на таксите за оценяване на съответствието съгласно член 43 се вземат предвид специфичните интереси и нужди на малките доставчици, като тези такси се намаляват пропорционално на техния размер и размера на пазара.

ДЯЛ VI

УПРАВЛЕНИЕ

ГЛАВА 1

ЕВРОПЕЙСКИ СЪВЕТ ПО ИЗКУСТВЕН ИНТЕЛЕКТ

Член 56

Създаване на Европейски съвет по изкуствен интелект

1. Създава се Европейски съвет по изкуствен интелект („Съвет по ИИ“).
2. Съветът по ИИ предоставя съвети и помощ на Комисията с цел да:
 - а) допринася за ефективното сътрудничество между националните надзорни органи и Комисията по въпросите, обхванати от настоящия регламент;
 - б) координира и допринася към насоките и анализа от Комисията и националните надзорни органи и други компетентни органи по нововъзникващи въпроси в рамките на вътрешния пазар по отношение на въпроси, обхванати от настоящия регламент;
 - в) подпомага националните надзорни органи и Комисията за осигуряване на последователното прилагане на настоящия регламент.

Член 57

Структура на Съвета по ИИ

1. Съветът по ИИ се състои от националните надзорни органи, които се представляват от ръководителя или равностойно високопоставено длъжностно лице на този орган, и от Европейския надзорен орган по защита на данните. Други национални органи могат да бъдат поканени на заседанията, когато обсъжданите въпроси са от значение за тях.
2. Съветът по ИИ приема свой процедурен правилник с обикновено мнозинство от членовете си след одобрение от Комисията. Процедурният правилник съдържа също така оперативните аспекти, свързани с изпълнението на задачите на Съвета по ИИ, изброени в член 58. Съветът по ИИ може да създава подгрупи, когато това е целесъобразно за разглеждането на конкретни въпроси.
3. Съветът по ИИ се председателства от Комисията. Комисията свиква заседанията и подготвя дневния ред в съответствие със задачите на Съвета по ИИ съгласно настоящия регламент и неговия процедурен правилник. Комисията предоставя административна и аналитична подкрепа за дейностите на Съвета по ИИ съгласно настоящия регламент.
4. Съветът по ИИ може да кани външни експерти и наблюдатели да присъстват на заседанията му и може да провежда обмен със заинтересовани трети страни, за да информира за своите дейности в подходяща степен. За тази цел Комисията може да улеснява обмена между Съвета по ИИ и други органи, служби, агенции и консултативни групи на Съюза.

Член 58
Задачи на Съвета по ИИ

Когато консултира и подпомага Комисията в контекста на член 56, параграф 2, Съветът по ИИ по-специално:

- a) събира и обменя експертен опит и най-добри практики сред държавите членки;
- б) допринася за единни административни практики в държавите членки, включително за функционирането на регулаторните лаборатории, посочени в член 53;
- в) издава становища, препоръки или писмени становища по въпроси, свързани с прилагането на настоящия регламент, и по-специално
 - i) относно техническите спецификации или съществуващите стандарти по отношение на изискванията, посочени в дял III, глава 2;
 - ii) относно използването на хармонизираните стандарти или общите спецификации, посочени в членове 40 и 41;
 - iii) относно изготвянето на ръководни документи, включително насоките относно определянето на административните глоби, посочени в член 71.

ГЛАВА 2

НАЦИОНАЛНИ КОМПЕТЕНТНИ ОРГАНИ

Член 59
Определяне на национални компетентни органи

1. Всяка държава членка създава или определя национални компетентни органи с цел да се гарантира прилагането и изпълнението на настоящия регламент. Националните компетентни органи имат организация, която гарантира обективността и безпристрастността на техните дейности и задачи.
2. Всяка държава членка определя национален надзорен орган измежду националните компетентни органи. Националният надзорен орган действа като нотифициращ орган и орган за надзор на пазара, освен ако държавата членка няма организационни и административни причини да определи повече от един орган.
3. Държавите членки информират Комисията за това кой или кои органи са били определени и, когато е приложимо, за причините да бъде определен повече от един орган.
4. Държавите членки гарантират, че националните компетентни органи разполагат с достатъчно финансови и човешки ресурси, за да изпълняват задачите си съгласно настоящия регламент. По-специално националните компетентни органи разполагат с достатъчен брой постоянно наличен персонал, чиято компетентност и експертен опит включват задълбочено разбиране на технологиите за изкуствен интелект, данните и компютърните системи за данни, основните права, рисковете за здравето и безопасността, както и познаване на съществуващите стандарти и правни изисквания.
5. Държавите членки докладват ежегодно на Комисията относно състоянието на финансовите и човешките ресурси на националните компетентни органи с

оценка на тяхната адекватност. Комисията предава тази информация на Съвета по ИИ за обсъждане и евентуални препоръки.

6. Комисията улеснява обмена на опит между националните компетентни органи.
7. Националните компетентни органи могат да предоставят насоки и съвети относно прилагането на настоящия регламент, включително на малки доставчици. Когато националните компетентни органи възнамеряват да предоставят насоки и съвети във връзка със система с ИИ в области, обхванати от друго законодателство на Съюза, по целесъобразност се провеждат консултации с националните органи, които са компетентни по въпросното законодателство на Съюза. Държавите членки могат също така да създадат едно централно звено за комуникация с операторите.
8. Когато институциите, агенциите и органите на Съюза попадат в обхвата на настоящия регламент, Европейският надзорен орган по защита на данните действа като компетентен орган за техния надзор.

ДЯЛ VII

БАЗА ДАННИ НА ЕС ЗА САМОСТОЯТЕЛНИ ВИСОКОРИСКОВИ СИСТЕМИ С ИИ

Член 60

База данни на ЕС за самостоятелни високорискови системи с ИИ

1. Комисията, в сътрудничество с държавите членки, създава и поддържа база данни на ЕС, съдържаща посочената в параграф 2 информация относно високорисковите системи с ИИ, упоменати в член 6, параграф 2, които са регистрирани в съответствие с член 51.
2. Данните, изброени в приложение VIII, се въвеждат в базата данни на ЕС от доставчиците. Комисията предоставя на последните техническа и административна подкрепа.
3. Информацията, съдържаща се в базата данни на ЕС, е достъпна за обществеността.
4. Базата данни на ЕС съдържа лични данни само доколкото това е необходимо за събирането и обработването на информация в съответствие с настоящия регламент. Тази информация включва имената и данните за контакт на физическите лица, които отговарят за регистрацията на системата и имат законното правомощие да представляват доставчика.
5. Комисията е администратор на базата данни на ЕС. Тя също така гарантира на доставчиците адекватна техническа и административна подкрепа.

ДЯЛ VIII

МОНИТОРИНГ СЛЕД ПУСКАНЕТО НА ПАЗАРА, ОБМЕН НА ИНФОРМАЦИЯ, НАДЗОР НА ПАЗАРА

ГЛАВА 1

МОНИТОРИНГ СЛЕД ПУСКАНЕТО НА ПАЗАРА

Член 61

Мониторинг от доставчиците след пускането на пазара и план за мониторинг след пускането на пазара за високорискови системи с ИИ

1. Доставчиците създават и документират система за мониторинг след пускането на пазара по начин, съобразен с естеството на технологиите за изкуствен интелект и с рисковете на високорисковата система с ИИ.
2. Системата за мониторинг след пускането на пазара активно и систематично събира, документира и анализира съответните данни, предоставени от ползвателите или събрани чрез други източници относно функционирането на високорисковите системи с ИИ през целия им жизнен цикъл, и позволява на доставчика да оценява непрекъснатото съответствие на системите с ИИ с изискванията, посочени в дял III, глава 2.
3. Системата за мониторинг след пускането на пазара се основава на план за мониторинг след пускането на пазара. Планът за мониторинг след пускане на пазара представлява част от техническата документация, посочена в приложение IV. Комисията приема акт за изпълнение за определяне на подробни разпоредби за установяване на образец на плана за мониторинг след пускането на пазара и списък на елементите, които трябва да бъдат включени в плана.
4. За високорисковите системи с ИИ, обхванати от правните актове, посочени в приложение II, когато съгласно това законодателство вече е създадена система и план за мониторинг след пускането на пазара, елементите, описани в параграфи 1, 2 и 3, се интегрират по целесъобразност в тази система и план.

Първа алинея се прилага и за високорисковите системи с ИИ, посочени в точка 5, буква б) от приложение III, които са пуснати на пазара или въведени в експлоатация от кредитни институции, регламентирани от Директива 2013/36/ЕС.

ГЛАВА 2

ОБМЕН НА ИНФОРМАЦИЯ ЗА ИНЦИДЕНТИ И НЕИЗПРАВНОСТИ

Член 62

Докладване на сериозни инциденти и неизправности

1. Доставчиците на високорискови системи с ИИ, пуснати на пазара на Съюза, докладват за всеки сериозен инцидент или неизправност на тези системи, които

представляват нарушение на задълженията съгласно правото на Съюза, предназначено да защитава основните права, пред органите за надзор на пазара на държавите членки, в които е възникнал инцидентът или нарушението.

Доставчикът извършва това уведомяване веднага щом установи причинно-следствена връзка между системата с ИИ и инцидента или неизправността или правдоподобна вероятност за такава връзка, и във всеки случай не по-късно от 15 дни, след като доставчиците са узнали за сериозния инцидент или за неизправността.

2. При получаване на уведомление, свързано с нарушение на задълженията съгласно правото на Съюза, предназначено да защитава основните права, органът за надзор на пазара информира националните публични органи или структури, посочени в член 64, параграф 3. Комисията разработва специални насоки за улесняване на спазването на задълженията, посочени в параграф 1. Тези насоки се издават най-късно 12 месеца след влизането в сила на настоящия регламент.
3. За високорисковите системи с ИИ, посочени в точка 5, буква б) от приложение III, които са пуснати на пазара или въведени в експлоатация от доставчици, които са кредитни институции, регулирани от Директива 2013/36/ЕС, и за високорисковите системи с ИИ, които са защитни елементи на устройства или сами по себе си устройства, попадащи в обхвата на Регламент (ЕС) 2017/745 и Регламент (ЕС) 2017/746, уведомяването за сериозни инциденти или неизправности се ограничава до тези, които представляват нарушение на задълженията съгласно правото на Съюза, предназначено да защитава основните права.

ГЛАВА 3

ПРАВОПРИЛАГАНЕ

Член 63

Надзор на пазара и контрол върху системите с ИИ на пазара на Съюза

1. По отношение на системите с ИИ, обхванати от настоящия регламент, се прилага Регламент (ЕС) 2019/1020. За целите на ефективното прилагане на настоящия регламент обаче:
 - а) всяко позоваване на икономически оператор съгласно Регламент (ЕС) 2019/1020 се разбира като включващо всички оператори, посочени в дял III, глава 3 от настоящия регламент;
 - б) всяко позоваване на продукт съгласно Регламент (ЕС) 2019/1020 се разбира като включващо всички системи с ИИ, попадащи в обхвата на настоящия регламент.
2. Националният надзорен орган докладва редовно на Комисията резултатите от съответните дейности по надзор на пазара. Националният надзорен орган докладва незабавно на Комисията и на съответните национални органи за защита на конкуренцията всяка информация, установена в хода на дейностите по надзор на пазара, която може да представлява потенциален интерес за прилагането на правото на Съюза в областта на правилата за конкуренция.

3. За високорисковите системи с ИИ, свързани с продукти, за които се прилагат правните актове, изброени в приложение II, раздел А, органът за надзор на пазара за целите на настоящия регламент е органът, отговарящ за дейностите по надзор на пазара, определен съгласно тези правни актове.
4. За системите с ИИ, пуснати на пазара, въведени в експлоатация или използвани от финансови институции, регулирани от законодателството на Съюза в областта на финансовите услуги, органът за надзор на пазара за целите на настоящия регламент е съответният орган, отговарящ за финансовия надзор на тези институции съгласно това законодателство.
5. За системите с ИИ, изброени в точка 1, буква а), доколкото системите се използват за целите на правоприлагането, и в точки 6 и 7 от приложение III, държавите членки определят за органи за надзор на пазара за целите на настоящия регламент или компетентните надзорни органи за защита на данните съгласно Директива (ЕС) 2016/680 или Регламент 2016/679, или националните компетентни органи, упражняващи надзор върху дейностите на правоприлагащите органи, имиграционните органи или органите в областта на убежището, които въвеждат в експлоатация или използват тези системи.
6. Когато институциите, агенциите и органите на Съюза попадат в обхвата на настоящия регламент, Европейският надзорен орган по защита на данните действа като техен компетентен орган за надзор на пазара.
7. Държавите членки улесняват координацията между органите за надзор на пазара, определени съгласно настоящия регламент, и други съответни национални органи или структури, които упражняват надзор върху прилагането на законодателството на Съюза за хармонизация, посочено в приложение II, или друго законодателство на Съюза, което може да е от значение за високорисковите системи с ИИ, посочени в приложение III.

Член 64

Достъп до данни и документи

1. На органите за надзор на пазара се предоставя пълен достъп до данните и документацията в контекста на техните дейности, до използваните от доставчика набори от данни за обучение, признаване и изпитване, включително чрез приложно-програмни интерфейси („API“) или други подходящи технически средства и инструменти, позволяващи дистанционен достъп.
2. Когато е необходимо да се оцени съответствието на високорисковата система с ИИ с изискванията, посочени в дял III, глава 2, и при обосновано искане, на органите за надзор на пазара се предоставя достъп до изходния код на системата с ИИ.
3. Националните публични органи или структури, които упражняват надзор или налагат спазването на задълженията съгласно правото на Съюза за защита на основните права във връзка с използването на високорисковите системи с ИИ, посочени в приложение III, имат правомощието да изискват и получават достъп до всяка документация, създадена или поддържана съгласно настоящия регламент, когато достъпът до тази документация е необходим за осъществяването на задачите им съгласно техните правомощия и в рамките на тяхната юрисдикция. Съответният публичен орган или структура информира

органа за надзор на пазара на съответната държава членка за всяко такова искане.

4. До 3 месеца след влизането в сила на настоящия регламент всяка държава членка определя публичните органи или структури, посочени в параграф 3, и публикува списък на уебсайта на националния надзорен орган. Държавите членки уведомяват Комисията и всички останали държави членки за списъка и го актуализират редовно.
5. Когато документацията, посочена в параграф 3, е недостатъчна, за да се установи дали е извършено нарушение на задълженията, произтичащи от правото на Съюза, предназначено да защитава основните права, публичният орган или структура, посочен(а) в параграф 3, може да отправи обосновано искане до органа за надзор на пазара да организира изпитване на високорисковата система с ИИ чрез технически средства. Органът за надзор на пазара организира изпитването с активното участие на отпращаващия искането публичен орган или структура в разумен срок след подаване на искането.
6. Всяка информация и документация, получени от националните публични органи или структури, посочени в параграф 3, съгласно разпоредбите на настоящия член, се третират в съответствие със задълженията за поверителност, посочени в член 70.

Член 65

Процедура при системи с ИИ, представляващи риск на национално равнище

1. Системите с ИИ, представляващи риск, се считат за продукт, представляващ риск по смисъла на член 3, точка 19 от Регламент (ЕС) 2019/1020, що се отнася до рисковете за здравето или безопасността или за защитата на основните права на хората.
2. Когато органът за надзор на пазара на държава членка има достатъчно основания да счита, че дадена система с ИИ представлява риск, както е посочено в параграф 1, той извършва оценяване на съответната система с ИИ по отношение на нейното съответствие с всички изисквания и задължения, определени в настоящия регламент. Когато са налице рискове за защитата на основните права, органът за надзор на пазара информира съответните национални публични органи или структури, посочени в член 64, параграф 3. Съответните оператори сътрудничат при необходимост на органите за надзор на пазара и на другите национални публични органи или структури, посочени в член 64, параграф 3.

Когато в хода на това оценяване органът за надзор на пазара констатира, че системата с ИИ не съответства на изискванията и задълженията, определени в настоящия регламент, той незабавно изисква от съответния оператор да предприеме всички необходими коригиращи действия, за да приведе в съответствие системата с ИИ, да я изтегли от пазара или да я изведе в съобразен с характера на риска разумен срок, който органът за надзор може да определи.

Органът за надзор на пазара надлежно информира съответния нотифициран орган. Прямо посочените във втора алинея мерки се прилага член 18 от Регламент (ЕС) 2019/1020.

3. Когато органът за надзор на пазара счита, че несъответствието не е ограничено само до националната му територия, той информира Комисията и другите държави членки за резултатите от оценяването и за действията, които той е изискал да бъдат предприети от оператора.
4. Операторът гарантира, че ще предприема всички подходящи коригиращи действия по отношение на всички засегнати системи с ИИ, които той е предоставил на пазара в целия Съюз.
5. Когато операторът на система с ИИ не предприеме подходящо коригиращо действие в посочения в параграф 2 срок, органът за надзор на пазара взема всички целесъобразни временни мерки, за да забрани или ограничи предоставянето на системата с ИИ на пазара на съответната държава членка или за да изтегли продукта от този пазар, или за да го из земе. Този орган незабавно информира Комисията и другите държави членки за тези мерки.
6. Информацията, посочена в параграф 5, включва всички налични подробни данни, по-специално данните, необходими за идентифицирането на несъответстващата система с ИИ, произхода на системата с ИИ, естеството на предполагаемото несъответствие и съпътстващия риск, естеството и продължителността на предприетите на национално равнище мерки, както и аргументите, изтъкнати от съответния оператор. По-специално органите за надзор на пазара посочват дали несъответствието се дължи на една или няколко от следните причини:
 - а) несъответствие на системата с ИИ с изискванията, посочени в дял III, глава 2;
 - б) недостатъци в хармонизираните стандарти или в общите спецификации, посочени в членове 40 и 41, на които се основава презумпцията за съответствие.
7. Органите за надзор на пазара на държавите членки, различни от органа за надзор на пазара на държавата членка, започнала процедурата, без забавяне информират Комисията и другите държави членки за всички приети мерки и за всяка допълнителна информация, с която разполагат за несъответствието на съответната система с ИИ, и в случай на несъгласие с нотифицираната национална мярка — за своите възражения.
8. Когато в срок от три месеца от получаването на информацията, посочена в параграф 5, не е повдигнато възражение нито от държава членка, нито от Комисията във връзка с временна мярка, предприета от държава членка, тази мярка се счита за обоснована. Това не засяга процедурните права на съответния оператор в съответствие с член 18 от Регламент (ЕС) 2019/1020.
9. Органите за надзор на пазара на всички държави членки гарантират, че без забавяне се вземат подходящите ограничителни мерки по отношение на въпросния продукт, като например изтеглянето на продукта от пазарите им.

Член 66

Предпазна процедура на Съюза

1. Когато в срок от три месеца след получаване на уведомлението по член 65, параграф 5 държава членка е повдигнала възражения срещу мярка, предприета от друга държава членка, или когато Комисията счита, че мярката противоречи

на правото на Съюза, тя незабавно започва консултации със съответната държава членка и съответния оператор или оператори и извършва оценка на тази национална мярка. Въз основа на резултатите от тази оценка Комисията решава дали националната мярка е оправдана или не в срок от 9 месеца от уведомяването, посочено в член 65, параграф 5, и уведомява съответната държава членка за това решение.

2. Ако бъде преценено, че националната мярка е обоснована, всички държави членки предприемат необходимите мерки, за да осигурят изтеглянето от своя пазар на несъответстващата система с ИИ и информират Комисията за това. Ако бъде преценено, че националната мярка не е обоснована, съответната държава членка оттегля мярката.
3. Когато се прецени, че националната мярка е обоснована и несъответствието на системата с ИИ се дължи на недостатъци в хармонизираните стандарти или общите спецификации, посочени в членове 40 и 41 от настоящия регламент, Комисията прилага процедурата, предвидена в член 11 от Регламент (ЕС) № 1025/2012.

Член 67

Съответстващи на изискванията системи с ИИ, които представляват риск

1. Когато орган за надзор на пазара на държава членка, след като извърши оценяването съгласно член 65, установи, че дадена система с ИИ, която отговаря на изискванията по настоящия регламент, въпреки това представлява риск за здравето и безопасността на хората, за спазването на задълженията съгласно правото на Съюза или националното право, предназначено да защитава основните права, или за други аспекти на защитата на обществен интерес, той изисква от съответния оператор да предприеме всички подходящи мерки, за да гарантира, че когато въпросната система с ИИ бъде пусната на пазара или въведена в експлоатация, тя няма да представлява този риск, да изтегли системата с ИИ от пазара или да я изведе в рамките на разумен, съобразен с характера на риска срок, който органът може да определи.
2. Доставчикът или други съответни оператори гарантират, че се предприемат коригиращи действия по отношение на въпросните системи с ИИ, които те са предоставили на пазара в целия Съюз, в рамките на срока, определен от органа за надзор на пазара на държавата членка, посочен в параграф 1.
3. Държавата членка незабавно информира Комисията и другите държави членки. Тази информация включва всички налични подробни данни, по-специално данните, необходими за идентифицирането на съответната система с ИИ, произхода и веригата на доставки на системата с ИИ, естеството на съпътстващия риск и естеството и продължителността на мерките, предприети на национално равнище.
4. Комисията незабавно започва консултации с държавите членки и съответния оператор и оценява предприетата национална мярка. Въз основа на резултатите от тази оценка Комисията взема решение дали мярката е оправдана или не и когато е необходимо, предлага подходящи мерки.
5. Комисията адресира решението си до държавите членки.

Член 68
Официално несъответствие

1. Когато органът за надзор на пазара на дадена държава членка направи някоя от следните констатации, той изисква от съответния доставчик да прекрати въпросното несъответствие:
 - а) маркировката за съответствие е нанесена в нарушение на член 49;
 - б) маркировката за съответствие не е нанесена;
 - в) декларацията за съответствие с изискванията на ЕС не е съставена;
 - г) декларацията за съответствие с изискванията на ЕС е съставена неправилно;
 - д) идентификационният номер на нотифицирания орган, участващ в процедурата за оценяване на съответствието, когато е приложимо, не е нанесен.
2. Когато несъответствието, посочено в параграф 1, продължи, съответната държава членка предприема всички подходящи мерки, за да ограничи или да забрани предоставянето на високорисковата система с ИИ на пазара или да осигури нейното изтегляне или изземване от пазара.

ДЯЛ IX

КОДЕКСИ ЗА ПОВЕДЕНИЕ

Член 69
Кодекси за поведение

1. Комисията и държавите членки насърчават и улесняват изготвянето на кодекси за поведение, предназначени да насърчават доброволното прилагане към системи с ИИ, различни от високорискови системи с ИИ, на изискванията, посочени в дял III, глава 2, въз основа на технически спецификации и решения, които са подходящи средства за гарантиране на спазването на тези изисквания с оглед на предназначението на системите.
2. Комисията и Съветът по ИИ насърчават и улесняват изготвянето на кодекси за поведение, предназначени да поощряват доброволното прилагане спрямо системите с ИИ на изисквания, свързани например с тяхната екосъобразност, достъпност за хората с увреждания, с участието на заинтересованите страни в тяхното проектиране и разработване и с културно-личностното разнообразие на екипите от разработчици въз основа на ясни цели и ключови показатели за ефективност за измерване на постигането на тези цели.
3. Кодексите за поведение могат да бъдат изготвени от отделни доставчици на системи с ИИ или от организации, които ги представляват, или съвместно от доставчици и техни представителни организации, включително с участието на ползватели и заинтересовани страни и техните представителни организации. Кодексите за поведение могат да обхващат една или повече системи с ИИ, като се отчита сходството в предназначението на съответните системи.

4. Комисията и Съветът по ИИ вземат предвид специфичните интереси и нужди на малките доставчици и стартиращите предприятия, когато насърчават и подпомагат изготвянето на кодекси за поведение.

ДЯЛ X

ПОВЕРИТЕЛНОСТ И САНКЦИИ

Член 70

Поверителност

1. Националните компетентни органи и нотифицираните органи, участващи в прилагането на настоящия регламент, зачитат поверителността на информацията и данните, получавани при изпълнение на техните задачи и дейности, така че да защитават по-специално:
- а) правата върху интелектуалната собственост и поверителната търговска информация или търговски тайни на дадено физическо или юридическо лице, включително изходния код, освен в случаите, посочени в член 5 от Директива 2016/943 относно защитата на неразкрити ноу-хау и търговска информация (търговски тайни) срещу тяхното незаконно придобиване, използване и разкриване;
 - б) ефективното прилагане на настоящия регламент, по-конкретно при проверките, разследванията или одитите;обществения интерес и националната сигурност;
 - в) независимостта на наказателните или административните производства.
2. Без да се засяга параграф 1, информацията, обменена на поверителна основа между националните компетентни органи и между националните компетентни органи и Комисията, не се разкрива без предварителна консултация с националния компетентен орган, който е изпратил първоначално въпросната информация, и с ползвателя, когато високорисковите системи с ИИ, посочени в точки 1, 6 и 7 от приложение III, се използват от правоприлагащите органи, имиграционните органи или органите в областта на убежището, когато такова разкриване би застрашило обществените интереси и националната сигурност.
- Когато правоприлагащите органи, имиграционните органи или органите в областта на убежището са доставчици на високорисковите системи с ИИ, посочени в точки 1, 6 и 7 от приложение III, техническата документация, посочена в приложение IV, остава в помещенията на тези органи. Тези органи гарантират, че органите за надзор на пазара, посочени в член 63, параграфи 5 и 6, според случая, могат при поискване незабавно да получат достъп до документацията или да получат копие от нея. Достъп до тази документация или получаване на копие от нея се разрешава само на персонала на органа за надзор на пазара, притежаващ съответното ниво на разрешение за достъп.
3. Параграфи 1 и 2 не засягат правата и задълженията на Комисията, държавите членки и нотифицираните органи по отношение на обмена на информация и разпространяването на предупреждения, нито задълженията на засегнатите страни за представяне на информация съгласно наказателното право на държавите членки.

4. Комисията и държавите членки могат при необходимост да обменят поверителна информация с регулаторните органи на трети държави, с които са сключили двустранни или многостранни споразумения, гарантиращи адекватно равнище на поверителност.

Член 71
Санкции

1. В съответствие с реда и условията, предвидени в настоящия регламент, държавите членки определят правилата относно санкциите, включително административните глоби, приложими при нарушения на настоящия регламент, и вземат всички необходими мерки, за да гарантират, че те се прилагат правилно и ефективно. Санкциите трябва да бъдат ефективни, съразмерни и възпиращи. При тях се вземат предвид по-специално интересите на малките доставчици и стартиращите предприятия и тяхната икономическа жизнеспособност.
2. Държавите членки уведомяват Комисията за тези разпоредби и мерки и я уведомяват незабавно за всяко последващо изменение, което ги засяга.
3. Следните нарушения подлежат на административни глоби в размер до 30 000 000 EUR или, ако нарушителят е дружество, до 6 % от общия му годишен световен оборот за предходната финансова година, в зависимост от това коя от двете суми е по-висока:
 - а) неспазване на забраната на практиките в сферата на изкуствения интелект, посочена в член 5;
 - б) несъответствие на системата с ИИ с изискванията, посочени в член 10.
4. Несъответствието на системата с ИИ с изисквания или задължения по настоящия регламент, различни от посочените в членове 5 и 10, подлежи на административни глоби в размер до 20 000 000 EUR или, ако нарушителят е дружество, до 4 % от общия му годишен световен оборот за предходната финансова година, в зависимост от това коя от двете суми е по-висока.
5. Предоставянето на неправилна, непълна или подвеждаща информация в отговор на искане от нотифицираните органи или националните компетентни органи подлежи на административни глоби в размер до 10 000 000 EUR или, ако нарушителят е дружество, до 2 % от общия му годишен световен оборот за предходната финансова година, в зависимост от това коя от двете суми е по-висока.
6. При вземането на решение относно размера на административната глоба във всеки отделен случай се вземат предвид всички обстоятелства от значение за конкретната ситуация и се обръща надлежно внимание на следното:
 - а) естеството, тежестта и продължителността на нарушението и последиците от него;
 - б) дали други органи за надзор на пазара вече са наложили административни глоби на същия оператор за същото нарушение;
 - в) размера и пазарния дял на оператора, извършил нарушението.

7. Всяка държава членка определя правила за това дали и до каква степен могат да бъдат налагани административни глоби на публични органи и структури, установени в тази държава членка.
8. В зависимост от правната система на държавите членки правилата относно административните глоби могат да се прилагат по такъв начин, че глобите да се налагат от компетентните национални съдилища или други органи според практиката в тези държави членки. Прилагането на тези правила в тези държави членки има равностоен ефект.

Член 72

Административни глоби на институциите, агенциите и органите на ЕС

1. Европейският надзорен орган по защита на данните може да налага административни глоби на институциите, агенциите и органите на Съюза, попадащи в обхвата на настоящия регламент. При вземането на решение дали да бъде наложена административна глоба и относно размера на административната глоба във всеки отделен случай се вземат предвид всички обстоятелства от значение за конкретната ситуация и се обръща надлежно внимание на следното:
 - а) естеството, тежестта и продължителността на нарушението и последиците от него;
 - б) сътрудничеството с Европейския надзорен орган по защита на данните с цел отстраняване на нарушението и ограничаване на евентуалните неблагоприятни последици от него, включително спазването на всяка от мерките, разпоредени по-рано от Европейския надзорен орган по защита на данните срещу съответната институция, агенция или орган на Съюза по същия предмет;
 - в) всички подобни предишни нарушения от страна на институцията, агенцията или органа на Съюза.
2. Следните нарушения подлежат на административни глоби в размер до 500 000 EUR:
 - а) неспазване на забраната на практиките в сферата на изкуствения интелект, посочена в член 5;
 - б) несъответствие на системата с ИИ с изискванията, посочени в член 10.
3. Несъответствието на системата с ИИ с изисквания или задължения по настоящия регламент, различни от посочените в членове 5 и 10, подлежи на административни глоби в размер до 250 000 EUR.
4. Преди да вземе решения съгласно настоящия член, Европейският надзорен орган по защита на данните дава на институцията, агенцията или органа на Съюза, по отношение на които се провеждат производствата от Европейския надзорен орган, възможността да бъдат изслушани във връзка с евентуално нарушение. Европейският надзорен орган по защита на данните основава своите решения единствено на данни и обстоятелства, по които засегнатите страни са имали възможност да изразят становище. Евентуалните жалбоподатели, ако има такива, се привличат за тясно сътрудничество по производството.

5. Правото на защита на засегнатите страни се съблюдава в хода на цялото производство. Те имат правото на достъп до преписката на Европейския надзорен орган по защита на данните, при условие че се зачита законният интерес на физическите лица или на предприятията за защита на техните лични данни или търговски тайни.
6. Средствата, събрани чрез налагането на имуществени санкции съгласно настоящия член, представляват приход в общия бюджет на Съюза.

ДЯЛ XI

ДЕЛЕГИРАНЕ НА ПРАВОМОЩИЕ И ПРОЦЕДУРА НА КОМИТЕТ

Член 73

Упражняване на делегирането

1. Правомощието да приема делегирани актове се предоставя на Комисията при спазване на предвидените в настоящия член условия.
2. Делегираното на правомощия, посочено в член 4, член 7, параграф 1, член 11, параграф 3, член 43, параграфи 5 и 6 и член 48, параграф 5, се предоставя на Комисията за неопределен срок, считано от [датата на влизане в сила на настоящия регламент].
3. Делегирането на правомощия, посочено в член 4, член 7, параграф 1, член 11, параграф 3, член 43, параграфи 5 и 6 и член 48, параграф 5, може да бъде оттеглено по всяко време от Европейския парламент или от Съвета. С решението за оттегляне се прекратява посоченото в него делегиране на правомощия. То поражда действие в деня след деня на публикуването му в *Официален вестник на Европейския съюз* или на по-късна, посочена в решението дата. Решението не засяга валидността на делегираните актове, които вече са в сила.
4. Веднага след като приеме делегиран акт, Комисията нотифицира акта едновременно на Европейския парламент и на Съвета.
5. Всеки делегиран акт, приет съгласно член 4, член 7, параграф 1, член 11, параграф 3, член 43, параграфи 5 и 6 и член 48, параграф 5, влиза в сила единствено ако нито Европейският парламент, нито Съветът не са представили възражения в срок от три месеца след нотифицирането на акта на Европейския парламент и Съвета или ако преди изтичането на този срок и Европейският парламент, и Съветът са уведомили Комисията, че няма да представят възражения. Посоченият срок се удължава с три месеца по инициатива на Европейския парламент или на Съвета.

Член 74

Процедура на комитет

1. Комисията се подпомага от комитет. Този комитет е комитет по смисъла на Регламент (ЕС) № 182/2011.
2. При позоваване на настоящия параграф се прилага член 5 от Регламент (ЕС) № 182/2011.

ДЯЛ XII

ЗАКЛЮЧИТЕЛНИ РАЗПОРЕДБИ

Член 75

Изменение на Регламент (ЕО) № 300/2008

В член 4, параграф 3 от Регламент (ЕО) № 300/2008 се добавя следната алинея:

„При приемането на подробни мерки, свързани с техническите спецификации и процедури за одобряване и използване на оборудване за сигурност по отношение на системи с изкуствен интелект по смисъла на Регламент (ЕС) YYY/XX [относно изкуствения интелект] на Европейския парламент и на Съвета*, се вземат предвид изискванията, определени в дял III, глава 2 от посочения регламент.

* Регламент (ЕС) YYY/XX [относно изкуствения интелект] (ОВ...)“

Член 76

Изменение на Регламент (ЕС) № 167/2013

В член 17, параграф 5 от Регламент (ЕС) № 167/2013 се добавя следната алинея:

„При приемането на делегирани актове съгласно първа алинея относно системи с изкуствен интелект, които представляват защитни елементи по смисъла на Регламент (ЕС) YYY/XX [относно изкуствения интелект] на Европейския парламент и на Съвета*, се вземат предвид изискванията, определени в дял III, глава 2 от посочения регламент.

* Регламент (ЕС) YYY/XX [относно изкуствения интелект] (ОВ...)“

Член 77

Изменение на Регламент (ЕС) № 168/2013

В член 22, параграф 5 от Регламент (ЕС) № 168/2013 се добавя следната алинея:

„При приемането на делегирани актове съгласно първа алинея относно системи с изкуствен интелект, които представляват защитни елементи по смисъла на Регламент (ЕС) YYY/XX относно [изкуствения интелект] на Европейския парламент и на Съвета*, се вземат предвид изискванията, установени в дял III, глава 2 от посочения регламент.

* Регламент (ЕС) YYY/XX [относно изкуствения интелект] (ОВ...)“

Член 78

Изменение на Директива 2014/90/ЕС

В член 8 от Директива 2014/90/ЕС се добавя следният параграф:

„4. За системите с изкуствен интелект, които представляват защитни елементи по смисъла на Регламент (ЕС) YYY/XX [относно изкуствения интелект] на Европейския парламент и на Съвета*, при извършването на дейностите си съгласно параграф 1 и при приемането на технически спецификации и стандарти за изпитване в съответствие с

параграфи 2 и 3 Комисията взема предвид изискванията, определени в дял III, глава 2 от посочения регламент.

* Регламент (ЕС) YYY/XX [относно изкуствения интелект] (ОВ...)“.

Член 79

Изменение на Директива (ЕС) 2016/797

В член 5 от Директива (ЕС) 2016/797 се добавя следният параграф:

„12. При приемането на делегирани актове съгласно параграф 1 и на актове за изпълнение съгласно параграф 11 относно системи с изкуствен интелект, които представляват защитни елементи по смисъла на Регламент (ЕС) YYY/XX [относно изкуствения интелект] на Европейския парламент и на Съвета*, се вземат предвид изискванията, установени в дял III, глава 2 от посочения регламент.

* Регламент (ЕС) YYY/XX [относно изкуствения интелект] (ОВ...)“.

Член 80

Изменение на Регламент (ЕС) 2018/858

В член 5 от Регламент (ЕС) 2018/858 се добавя следният параграф:

„4. При приемането на делегирани актове съгласно параграф 3 относно системи с изкуствен интелект, които представляват защитни елементи по смисъла на Регламент (ЕС) YYY/XX [относно изкуствения интелект] на Европейския парламент и на Съвета*, се вземат предвид изискванията, определени в дял III, глава 2 от посочения регламент.

* Регламент (ЕС) YYY/XX [относно изкуствения интелект] (ОВ...)“.

Член 81

Изменение на Регламент (ЕС) 2018/1139

Регламент (ЕС) 2018/1139 се изменя, както следва:

(1) В член 17 се добавя следният параграф:

„3. „Без да се засяга параграф 2, при приемането на актове за изпълнение съгласно параграф 1 относно системи с изкуствен интелект, които представляват защитни елементи по смисъла на Регламент (ЕС) YYY/XX [*относно изкуствения интелект*] на Европейския парламент и на Съвета*, се вземат предвид изискванията, определени в дял III, глава 2 от посочения регламент.

* Регламент (ЕС) YYY/XX [относно изкуствения интелект] (ОВ...)“.

(2) В член 19 се добавя следният параграф:

„4. При приемането на делегирани актове съгласно параграфи 1 и 2 относно системи с изкуствен интелект, които представляват защитни елементи по смисъла на Регламент (ЕС) YYY/XX [относно изкуствения интелект], се вземат предвид изискванията, определени в дял III, глава 2 от посочения регламент.“

(3) В член 43 се добавя следният параграф:

„4. При приемането на актове за изпълнение съгласно параграф 1 относно системи с изкуствен интелект, които представляват защитни елементи по смисъла на Регламент (ЕС) YYY/XX [относно изкуствения интелект], се вземат предвид изискванията, определени в дял III, глава 2 от посочения регламент.“

(4) В член 47 се добавя следният параграф:

„3. При приемането на делегирани актове съгласно параграфи 1 и 2 относно системи с изкуствен интелект, които представляват защитни елементи по смисъла на Регламент (ЕС) YYY/XX [относно изкуствения интелект], се вземат предвид изискванията, определени в дял III, глава 2 от посочения регламент.“

(5) В член 57 се добавя следният параграф:

„При приемането на тези актове за изпълнение относно системи с изкуствен интелект, които представляват защитни елементи по смисъла на Регламент (ЕС) YYY/XX [относно изкуствения интелект], се вземат предвид изискванията, определени в дял III, глава 2 от посочения регламент.“

(6) В член 58 се добавя следният параграф:

„3. При приемането на делегирани актове съгласно параграфи 1 и 2 относно системи с изкуствен интелект, които представляват защитни елементи по смисъла на Регламент (ЕС) YYY/XX [относно изкуствения интелект], се вземат предвид изискванията, определени в дял III, глава 2 от посочения регламент.“

Член 82

Изменение на Регламент (ЕС) 2019/2144

В член 11 от Регламент (ЕС) 2019/2144 се добавя следният параграф:

„3. При приемането на актовете за изпълнение съгласно параграф 2 относно системи с изкуствен интелект, които представляват защитни елементи по смисъла на Регламент (ЕС) YYY/XX [относно изкуствения интелект] на Европейския парламент и на Съвета*, се вземат предвид изискванията, определени в дял III, глава 2 от посочения регламент.

* Регламент (ЕС) YYY/XX [относно изкуствения интелект] (ОВ...)“.

Член 83

Системи с ИИ, които вече са пуснати на пазара или въведени в експлоатация

1. Настоящият регламент не се прилага за системи с ИИ, които са компоненти на широкомащабните информационни системи, създадени с правните актове, изброени в приложение IX, които са пуснати на пазара или въведени в експлоатация преди [12 месеца след началната дата на прилагане на настоящия регламент, посочена в член 85, параграф 2], освен ако замяната или изменението на тези правни актове не води до значителна промяна в проекта или предназначението на съответната система или системи с ИИ.

Изискванията, определени в настоящия регламент, се вземат предвид, когато е приложимо, при оценката на всяка широкомащабна информационна система, създадена с правните актове, изброени в приложение IX, която трябва да бъде предприета съгласно предвиденото в съответните актове.

2. Настоящият регламент се прилага за високорисковите системи с ИИ, различни от посочените в параграф 1, които са пуснати на пазара или въведени в експлоатация преди *[началната дата на прилагане на настоящия регламент, посочена в член 85, параграф 2]*, само ако от посочената дата тези системи претърпяват значителни промени в проекта или предназначението си.

Член 84

Оценка и преглед

1. след влизането в сила на настоящия регламент Комисията оценява веднъж годишно необходимостта от изменение на списъка в приложение III.
2. В срок до *[три години след началната дата на прилагане на настоящия регламент, посочена в член 85, параграф 2]* и на всеки четири години след това, Комисията представя на Европейския парламент и на Съвета доклад относно оценката и прегледа на настоящия регламент. Тези доклади се публикуват.
3. В докладите, посочени в параграф 2, се отделя специално внимание на следното:
 - а) състоянието на финансовите и човешките ресурси на националните компетентни органи с оглед на ефективното изпълнение на задачите, които са им възложени съгласно настоящия регламент;
 - б) санкциите, и по-специално административните глоби, посочени в член 71, параграф 1, налагани от държавите членки за нарушения на разпоредбите на настоящия регламент.
4. В срок от *[три години след началната дата на прилагане на настоящия регламент, посочена в член 85, параграф 2]* и на всеки четири години след това Комисията оценява въздействието и ефективността на кодексите за поведение с цел насърчаване на прилагането на изискванията, посочени в дял III, глава 2, и евентуално на други допълнителни изисквания за системите с ИИ, различни от високорисковите системи с ИИ.
5. Съветът по ИИ, държавите членки и националните компетентни органи предоставят на Комисията информация по нейно искане за целите на параграфи 1—4.
6. При извършването на оценките и прегледите по параграфи 1—4 Комисията взема предвид позициите и констатациите на Европейския съвет по изкуствен интелект, Европейския парламент, Съвета и на други компетентни органи или източници.
7. При необходимост Комисията представя подходящи предложения за изменение на настоящия регламент, като отчита по-специално развитието на технологиите и напредъка на информационното общество.

Член 85

Влизане в сила и прилагане

1. Настоящият регламент влиза в сила на двадесетия ден след публикуването му в *Официален вестник на Европейския съюз*.
2. Настоящият регламент се прилага от *[24 месеца след влизането му в сила]*.

3. Чрез дерогация от параграф 2:
- а) Дял III, глава 4 и дял VI се прилагат от [три месеца след влизането в сила на настоящия регламент];
 - б) Член 71 се прилага от [дванадесет месеца след влизането в сила на настоящия регламент].

Настоящият регламент е задължителен в своята цялост и се прилага пряко във всички държави членки.

Съставено в Брюксел на [...] година.

За Европейския парламент
Председател

За Съвета
Председател

ЗАКОНОДАТЕЛНА ФИНАНСОВА ОБОСНОВКА

1. РАМКА НА ПРЕДЛОЖЕНИЕТО/ИНИЦИАТИВАТА

- 1.1. Наименование на предложението/инициативата
- 1.2. Съответни области на политиката
- 1.3. Предложението/инициативата е във връзка с:
- 1.4. Цели
 - 1.4.1. Общи цели
 - 1.4.2. Конкретни цели
 - 1.4.3. Очаквани резултати и отражение
 - 1.4.4. Показатели за изпълнението
- 1.5. Мотиви за предложението/инициативата
 - 1.5.1. Изисквания, които трябва да бъдат изпълнени в краткосрочна или дългосрочна перспектива, включително подробен график за изпълнението на инициативата
 - 1.5.2. Добавена стойност от участието на Съюза (може да е в резултат от различни фактори, например ползи по отношение на координацията, правна сигурност, по-добра ефективност или взаимно допълване). За целите на тази точка „добавена стойност от участието на Съюза“ е стойността, която е резултат от намесата на ЕС и е допълнителна спрямо стойността, която би била създадена само от отделните държави членки
 - 1.5.3. Изводи от подобен опит в миналото
 - 1.5.4. Съвместимост с многогодишната финансова рамка и евентуални синергии с други подходящи инструменти
 - 1.5.5 Оценка на различните налични варианти за финансиране, включително възможностите за преразпределяне на средства
- 1.6. Продължителност и финансово отражение на предложението/инициативата
- 1.7. Планирани методи на управление

2. МЕРКИ ЗА УПРАВЛЕНИЕ

- 2.1. Правила за мониторинг и докладване
- 2.2. Система за управление и контрол
 - 2.2.1. Обосновка на предложените начини за управление, механизми за финансиране на изпълнението, начини за плащане и стратегия за контрол
 - 2.2.2. Информация относно установените рискове и системите за вътрешен контрол, създадени с цел намаляването им
 - 2.2.3. Оценка и обосновка на разходната ефективност на проверките (съотношение „разходи за контрол ÷ стойност на съответните управлявани фондове“) и оценка на очакваната степен на риска от грешки (при плащане и при приключване)

2.3. Мерки за предотвратяване на измами и нередности

3. ОЧАКВАНО ФИНАНСОВО ОТРАЖЕНИЕ НА ПРЕДЛОЖЕНИЕТО/ИНИЦИАТИВАТА

3.1. Съответни функции от многогодишната финансова рамка и разходни бюджетни редове

3.2. Очаквано финансово отражение на предложението върху бюджетните кредити

3.2.1. Обобщение на очакваното отражение върху бюджетните кредити за оперативни разходи

3.2.2. Очакван резултат, финансиран с бюджетни кредити за оперативни разходи

3.2.3. Обобщение на очакваното отражение върху бюджетните кредити за административни разходи

3.2.4. Съвместимост с настоящата многогодишна финансова рамка

3.2.5. Финансов принос от трети страни

3.3. Очаквано отражение върху приходите

ЗАКОНОДАТЕЛНА ФИНАНСОВА ОБОСНОВКА

1. РАМКА НА ПРЕДЛОЖЕНИЕТО/ИНИЦИАТИВАТА

1.1. Наименование на предложението/инициативата

Регламент на Европейския парламент и на Съвета за определяне на хармонизирани правила относно изкуствения интелект (Законодателен акт за изкуствения интелект) и за изменение на някои законодателни актове на Съюза

1.2. Съответни области на политиката

Съобщителни мрежи, съдържание и технологии;
Вътрешен пазар, промишленост, предприемачество и МСП;
Отражението върху бюджета се отнася до новите задачи, които са поверени на Комисията, включително подкрепата за Съвета на ЕС за изкуствения интелект.
Дейност: Изграждане на европейското цифрово бъдеще.

1.3. Предложението/инициативата е във връзка с:

Хново действие

- ново действие след пилотен проект/подготвително действие⁶⁴
- продължаване на съществуващо действие
- действие, пренасочено към ново действие

1.4. Цели

1.4.1. Общи цели

Общата цел на интервенцията е да се гарантира правилното функциониране на единния пазар чрез създаване на условия за разработването и използването на надежден изкуствен интелект в Съюза.

1.4.2. Конкретни цели

Конкретна цел № 1

Да се определят специфични за системите с ИИ изисквания и задължения по отношение на всички участници във веригата за създаване на стойност, за да се гарантира, че системите с ИИ, които се пускат на пазара и се използват, са безопасни и в съответствие с действащото законодателство в областта на основните права и ценностите на Съюза;

Конкретна цел № 2

Да се осигури правна сигурност, за да се улеснят инвестициите и иновациите в ИИ, като се изясни какви съществени изисквания, задължения, както и процедури за съответствие трябва да се спазват, за да се пусне на пазара или използва в Съюза дадена система с ИИ;

Конкретна цел № 3

⁶⁴

Съгласно член 54, параграф 2, буква а) или б) от Финансовия

Да се подобри управлението и ефективното прилагане на съществуващата правна уредба в областта на основните права и изискванията за безопасност, приложими към системите с ИИ, чрез предвиждане на нови правомощия, ресурси и ясни правила за съответните органи относно процедурите за оценяване на съответствието и за последващ мониторинг, както и разделение на задачите по управление и надзор между националното равнище и равнището на ЕС;

Конкретна цел № 4

Да се улесни развитието на единен пазар за законни, безопасни и надеждни приложения с ИИ и да се предотврати разпокъсаност на пазара чрез предприемане на действия от страна на ЕС за определяне на минимални изисквания за системите с ИИ, които могат да бъдат пускани на пазара и използвани в Съюза в съответствие с действащото законодателство в областта на основните права и безопасността.

1.4.3. Очаквани резултати и отражение

Да се посочи въздействието, което предложението/инициативата следва да окаже по отношение на бенефициерите/целевите групи.

Доставчиците на ИИ следва да се ползват от минимален, но ясен набор от изисквания, създаващи правна сигурност и гарантиращи достъп до целия единен пазар.

Ползвателите на ИИ следва да се ползват от правна сигурност, че високорисковите системи с ИИ, които купуват, са в съответствие с европейското законодателство и ценности.

Ползата за потребителите следва да бъде намален риск от компрометиране на тяхната безопасност или нарушаване на основните им права.

1.4.4. Показатели за изпълнението

Да се посочат показателите, които позволяват да се проследи изпълнението на предложението/инициативата.

Показател 1

Брой на сериозните злополуки или случаи на действие на ИИ, които представляват сериозен инцидент или нарушение на задълженията в областта на основните права (на шест месеца) по области на приложение и изчислени: а) в абсолютно изражение, б) като дял на внедрените приложения и в) като дял на засегнатите граждани.

Показател 2

а) Общо инвестиции в ИИ в ЕС (годишно)

б) Общо инвестиции в ИИ по държави членки (годишно)

в) Дял на дружествата, използващи ИИ (годишно)

г) Дял на МСП, използващи ИИ (годишно)

а) и б) ще се изчисляват въз основа на официални източници и ще бъдат съпоставени с частни оценки.

в) и г) ще се събрат чрез редовни анкети сред дружествата

1.5. Мотиви за предложението/инициативата

1.5.1. Изисквания, които трябва да бъдат изпълнени в краткосрочна или дългосрочна перспектива, включително подробен график за изпълнението на инициативата

Регламентът следва да започне да се прилага изцяло една година и половина след приемането му. Преди това обаче следва да бъдат изградени елементите на управленската структура. По-специално държавите членки трябва да са определили съществуващи органи и/или да са създали нови органи, които да изпълняват задачите, определени в законодателството, а Съветът на ЕС по ИИ следва да бъде сформиран и ефективно действащ. Към момента на началото на прилагането на регламента европейската база данни за системите с ИИ следва да функционира пълноценно. Следователно успоредно с процеса на приемане е необходимо да се разработи базата данни, така че нейното разработване да е завършено до влизането в сила на регламента.

- 1.5.2. *Добавена стойност от участието на Съюза (може да е в резултат от различни фактори, например ползи по отношение на координацията, правна сигурност, по-добра ефективност или взаимно допълване). За целите на тази точка „добавена стойност от участието на Съюза“ е стойността, която е резултат от намесата на ЕС и е допълнителна спрямо стойността, която би била създадена само от отделните държави членки.*

Една нововъзникваща разпокъсана рамка от потенциално разминаващи се национални правила ще възпрепятства безпроблемното предоставяне на системи с ИИ в целия ЕС и е неефективна като гаранция на безопасността и защитата на основните права и ценностите на Съюза в различните държави членки. Едно общо законодателно действие на ЕС в областта на ИИ би стимулирало вътрешния пазар и има голям потенциал да осигури на европейската промишленост конкурентно предимство на световната сцена и икономии от мащаба, които не могат да бъдат постигнати самостоятелно от отделните държави членки.

- 1.5.3. *Изводи от подобен опит в миналото*

С Директивата 2000/31/ЕО за електронната търговия се задава основната рамка за функционирането на единния пазар и надзора на цифровите услуги и се определя основната структура за общ механизъм за сътрудничество между държавите членки, обхващащ като цяло всички изисквания, приложими по отношение на цифровите услуги. При оценката на директивата бяха изтъкнати недостатъци на въпросния механизъм за сътрудничество в няколко аспекта, включително важни процесуални аспекти, като например липсата на ясни срокове за отговор от държавите членки, в съчетание с обща липса на реакция по отношение на искания от техни колеги. С течение на годините това доведе до липса на доверие между държавите членки при преодоляването на опасения във връзка с доставчиците, предлагащи трансгранични цифрови услуги. Оценката на директивата показва необходимостта от определяне на диференциран набор от правила и изисквания на европейско равнище. Поради тази причина изпълнението на специфичните задължения, определени в настоящия регламент, ще изисква специален механизъм за сътрудничество на равнището на ЕС с управленска структура, осигуряваща координация на конкретни отговорни органи на равнището на ЕС.

- 1.5.4. *Съвместимост с многогодишната финансова рамка и евентуални синергии с други подходящи инструменти*

Регламентът за определяне на хармонизирани правила за изкуствения интелект и за изменение на някои законодателни актове на Съюза определя нова обща рамка от изисквания, приложими към системите с ИИ, която далеч надхвърля рамката, предвидена от действащото законодателство. Поради тази причина с настоящото предложение трябва да се създаде нова национална и европейска регулаторна и координационна функция.

Що се отнася до възможните синергии с други подходящи инструменти, ролята на нотифициращите органи на национално равнище може да бъде изпълнявана от националните органи, изпълняващи подобни функции съгласно други регламенти на ЕС.

Освен това, като повишава доверието в ИИ и по този начин насърчава инвестициите в разработването и внедряването на ИИ, предложението за

регламент допълва „Цифрова Европа“, за която насърчаването на разпространението на ИИ е един от нейните пет приоритета.

1.5.5. Оценка на различните налични варианти за финансиране, включително възможностите за преразпределяне на средства

Служителите ще бъдат преразпределени. Останалите разходи ще бъдат подкрепени от пакета за програмата „Цифрова Европа“, като се има предвид, че целта на настоящия регламент – гарантиране на надежден ИИ – допринася пряко за една от ключовите цели на „Цифрова Европа“ – ускоряване на разработването и внедряването на ИИ в Европа.

1.6. Продължителност и финансово отражение на предложението/инициативата

ограничен срок на действие

- в сила от [ДД/ММ]ГГГГ до [ДД/ММ]ГГГГ
- Финансово отражение от ГГГГ до ГГГГ за бюджетни кредити за поети задължения и от ГГГГ до ГГГГ за бюджетни кредити за плащания.

Хнеограничен срок на действие

- Изпълнение с период на започване на дейност от една/две години (предстои потвърждение),
- последван от функциониране с пълен капацитет.

1.7. Планирани методи на управление⁶⁵

ХПряко управление от Комисията

- от нейните служби, включително от нейния персонал в делегациите на Съюза;
- от изпълнителните агенции

Споделено управление с държавите членки

Непряко управление чрез възлагане на задачи по изпълнението на бюджета на:

- трети държави или на органите, определени от тях;
 - международни организации и техните агенции (да се уточни);
 - ЕИБ и Европейския инвестиционен фонд;
 - органите, посочени в членове 70 и 71 от Финансовия регламент;
 - публичноправни органи;
 - частноправни органи със задължение за обществена услуга, доколкото са им предоставени подходящи финансови гаранции;
 - органи, уредени в частното право на държава членка, на които е възложено осъществяването на публично-частно партньорство и на които са предоставени подходящи финансови гаранции;
 - лица, на които е възложено изпълнението на специфични дейности в областта на ОВППС съгласно дял V от ДЕС и които са посочени в съответния основен акт.
- Ако е посочен повече от един метод на управление, пояснете в частта „Забележки“.

Забележки

⁶⁵ Подробности във връзка с методите на управление и позоваванията на Финансовия регламент могат да бъдат намерени на уебсайта BudgWeb: http://www.cc.cec/budg/man/budgmanag/budgmanag_en.html

2. МЕРКИ ЗА УПРАВЛЕНИЕ

2.1. Правила за мониторинг и докладване

Да се посочат честотата и условията.

Регламентът ще бъде преразгледан и оценен пет години след влизането му в сила. Комисията ще докладва за констатациите от оценката на Европейския парламент, Съвета и Европейския икономически и социален комитет.

2.2. Системи за управление и контрол

2.2.1. Обосновка на предложените начини за управление, механизми за финансиране на изпълнението, начини за плащане и стратегия за контрол

С регламента се установява нова политика по отношение на хармонизираните правила за предоставяне на системи с изкуствен интелект на вътрешния пазар, като същевременно се гарантира спазването на безопасността и основните права. Тези нови правила изискват механизъм за съгласуваност при трансграничното прилагане на задълженията по настоящия регламент под формата на нова консултативна група, която да координира дейностите на националните органи.

За да се отговори на тези нови задачи, е необходимо да се осигурят подходящи ресурси за службите на Комисията. Очаква се прилагането на новия регламент да изисква 10 ЕПРВ (5 ЕПРВ за подкрепа на дейностите на Съвета и 5 ЕПРВ за Европейския надзорен орган по защита на данните в качеството му на нотифициращ орган за системи с ИИ, внедрени от орган на Европейския съюз).

2.2.2. Информация относно установените рискове и системите за вътрешен контрол, създадени с цел намаляването им

За да се гарантира, че членовете на Съвета имат възможност да правят информиран анализ въз основа на фактически доказателства, се предвижда той да бъде подпомаган от административната структура на Комисията и да бъде създадена експертна група, която да предоставя допълнителен експертен опит, когато това е необходимо.

2.2.3. Оценка и обосновка на разходната ефективност на проверките (съотношение „разходи за контрол ÷ стойност на съответните управлявани фондове“) и оценка на очакваната степен на риска от грешки (при плащане и при приключване)

Като се има предвид ниската стойност на една трансакция (напр. възстановяване на пътните разходи на делегат за заседание), стандартните процедури за контрол изглеждат достатъчни за разходите за заседания. Що се отнася до разработването на базата данни, възлагането на договори е подкрепено от стабилна система за вътрешен контрол в ГД „Съобщителни мрежи, съдържание и технологии“ чрез централизираните дейности по възлагане на обществени поръчки.

2.3. Мерки за предотвратяване на измами и нередности

Да се посочат съществуващите или планираните мерки за превенция и защита, например от стратегията за борба с измамите.

Съществуващите мерки за превенция на измами, приложими за Комисията, ще покрият допълнителните бюджетни кредити, необходими за настоящия регламент.

3. ОЧАКВАНО ФИНАНСОВО ОТРАЖЕНИЕ НА ПРЕДЛОЖЕНИЕТО/ИНИЦИАТИВАТА

3.1. Съответни функции от многогодишната финансова рамка и разходни бюджетни редове

- Съществуващи бюджетни редове

По реда на функциите от многогодишната финансова рамка и на бюджетните редове.

Функция от многогодишната финансова рамка	Бюджетен ред	Вид на разхода	Финансов принос			
	Номер	Многогод. / едногод. ⁶⁶	от държави от ЕАСТ ⁶⁷	от държав и кандидати ⁶⁸	от трети държави	по смисъла на член 21, параграф 2, буква б) от Финансовия регламент
7	20 02 06 Административни разходи	Едногод.	НЕ	НЕ	НЕ	НЕ
1	02 04 03 „Цифрова Европа“ Изкуствен интелект	Многогод. д.	ДА	НЕ	НЕ	НЕ
1	02 01 30 01 Разходи за подкрепа на програмата „Цифрова Европа“	Едногод.	ДА	НЕ	НЕ	НЕ

⁶⁶ Многогод. = Многогодишни бюджетни кредити / Едногод. = Едногодишни бюджетни кредити

⁶⁷ ЕАСТ: Европейска асоциация за свободна търговия.

⁶⁸ Държави кандидатки и, ако е приложимо, потенциални кандидатки от Западните Балкани.

3.2. Очаквано финансово отражение на предложението върху бюджетните кредити

3.2.1. Обобщение на очакваното отражение върху бюджетните кредити за оперативни разходи

- Предложението/инициативата не налага използване на бюджетни кредити за оперативни разходи
- Предложението/инициативата налага използване на бюджетни кредити за оперативни разходи съгласно обяснението по-долу:

млн. евро (до 3-тия знак след десетичната запетая)

Функция от многогодишната финансова рамка	1	
--	---	--

ГД: CNECT				Година 2022	Година 2023	Година 2024	Година 2025	Година 2026	Година 2027 ⁶⁹	ОБЩО
• Бюджетни кредити за оперативни разходи										
Бюджетен ред ⁷⁰ 02 04 03	Поети задължения	(1a)		1,000						1,000
	Плащания	(2 a)		0,600	0,100	0,100	0,100	0,100		1,000
Бюджетен ред	Поети задължения	(1б)								
	Плащания	(2б)								
Бюджетни кредити за административни разходи, финансирани от пакета за определени програми ⁷¹										
Бюджетен ред 02 01 30 01		(3)		0,240	0,240	0,240	0,240	0,240	0,240	1,200

⁶⁹ Ориентировъчен и в зависимост от наличните бюджетни средства.

⁷⁰ Съгласно официалната бюджетна номенклатура.

⁷¹ Техническа и/или административна помощ и разходи в подкрепа на изпълнението на програми и/или дейности на ЕС (пришни редове ВА), непреки научни изследвания, преки научни изследвания.

ОБЩО бюджетни кредити за ГД СNECT	Поети задължения	=1a+16+3		1,240		0,240	0,240	0,240		2,200
	Плащания	=2a+2б +3		0,840	0,340	0,340	0,340	0,340		2,200

•ОБЩО бюджетни кредити за оперативни разходи	Поети задължения	(4)		1,000						1,000
	Плащания	(5)		0,600	0,100	0,100	0,100	0,100		1,000
•ОБЩО бюджетни кредити за административни разходи, финансирани от пакета за определени програми		(6)		0,240	0,240	0,240	0,240	0,240		1,200
ОБЩО бюджетни кредити за ФУНКЦИЯ 1 от многогодишната финансова рамка	Поети задължения	=4+ 6		1,240	0,240	0,240	0,240	0,240		2,200
	Плащания	=5+ 6		0,840	0,340	0,340	0,340	0,340		2,200

Ако предложението/инициативата има отражение върху повече от една функция, да се повтори частта по-горе:

•ОБЩО бюджетни кредити за оперативни разходи (всички оперативни функции)	Поети задължения	(4)								
	Плащания	(5)								
•ОБЩО бюджетни кредити за административни разходи, финансирани от пакета за определени програми (всички оперативни функции)		(6)								
ОБЩО бюджетни кредити за ФУНКЦИИ 1—6 от многогодишната финансова рамка (Референтна стойност)	Поети задължения	=4+ 6								
	Плащания	=5+ 6								

Функция от многогодишната финансова рамка	7	„Административни разходи“
--	----------	---------------------------

Тази част следва да бъде попълнена, като се използва таблицата за бюджетни данни от административно естество, която най-напред се въвежда в [приложението към законодателната финансова обосновка](#) (приложение V към вътрешните правила), което се качва в DECIDE за провеждането на вътрешни консултации между службите.

млн. евро (до 3-тия знак след десетичната запетая)

		Година 2023	Година 2024	Година 2025	Година 2026	Година 2027	След 2027 г. 72	ОБЩО
ГД: CNECT								
•Човешки ресурси		0,760	0,760	0,760	0,760	0,760	0,760	3,800
•Други административни разходи		0,010	0,010	0,010	0,010	0,010	0,010	0,050
ОБЩО за ГД CNECT		0,760	0,760	0,760	0,760	0,760	0,760	3,850
Европейски надзорен орган по защита на данните								
•Човешки ресурси		0,760	0,760	0,760	0,760	0,760	0,760	3,800
•Други административни разходи								
ОБЩО ЕНОЗД		0,760	0,760	0,760	0,760	0,760	0,760	3,800
ОБЩО бюджетни кредити за ФУНКЦИЯ 7 от многогодишната финансова рамка								
(Общо поети задължения = Общо плащания)		1,530	1,530	1,530	1,530	1,530	1,530	7,650

млн. евро (до 3-тия знак след десетичната запетая)

72

Всички цифри в тази колона са ориентировъчни и зависят от продължаването на програмите и наличието на бюджетни кредити.

		Година 2022	Година 2023	Година 2024	Година 2025	Година 2026	Година 2027		ОБЩО
ОБЩО бюджетни кредити за ФУНКЦИИ 1—7 от многогодишната финансова рамка	Поети задължения		2,770	1,770	1,770	1,770	1,770		9,850
	Плащания		2,370	1,870	1,870	1,870	1,870		9,850

3.2.2. Очакван резултат, финансиран с бюджетни кредити за оперативни разходи

Бюджетни кредити за поети задължения в милиони евро (до 3-тия знак след десетичната запетая)

Да се посочат целите и резултатите ↓			Година 2022		Година 2023		Година 2024		Година 2025		Година 2026		Година 2027		След 2027 ⁷³	ОБЩО		
			№	Разходи	№	Разходи	№	Разходи	№	Разходи	№	Разходи	№	Разходи	№	Разходи	Общ бр.	Общо разходи
РЕЗУЛТАТИ																		
КОНКРЕТНА ЦЕЛ № 1 ⁷⁴ ...																		
База данни					1	1,000	1		1		1		1		1	0,100	1	1,000
Заседания –					10	0,200	10	0,200	10	0,200	10	0,200	10	0,200	10	0,200	50	1,000
Информационни дейности					2	0,040	2	0,040	2	0,040	2	0,040	2	0,040	2	0,040	10	0,040
Междинен сбор за конкретна цел № 1																		
КОНКРЕТНА ЦЕЛ № 2...																		
- Резултат																		
Междинен сбор за конкретна цел № 2																		
ОБЩО					13	0,240	13	0,240	13	0,240	13	0,240	13	0,240	13	0,100	65	2,200

⁷³

Всички цифри в тази колона са ориентировъчни и зависят от продължаването на програмите и наличието на бюджетни кредити.

⁷⁴

Описана в точка 1.4.2. „Конкретни цели...“

3.2.3. *Обобщение на очакваното отражение върху бюджетните кредити за административни разходи*

- Предложението/инициативата не налага използване на бюджетни кредити за административни разходи
- Предложението/инициативата налага използване на бюджетни кредити за административни разходи съгласно обяснението по-долу:

млн. евро (до 3-тия знак след десетичната запетая)

	Година 2022	Година 2023	Година 2024	Година 2025	Година 2026	Година 2027	Годишно след 2027 ⁷⁵	ОБЩО
--	----------------	----------------	----------------	----------------	----------------	----------------	---------------------------------------	------

ФУНКЦИЯ 7 от многогодишната финансова рамка								
Човешки ресурси		1,520	1,520	1,520	1,520	1,520	1,520	7,600
Други административни разходи		0,010	0,010	0,010	0,010	0,010	0,010	0,050
Междинен сбор за ФУНКЦИЯ 7 от многогодишната финансова рамка		1,530	1,530	1,530	1,530	1,530	1,530	7,650

Извън ФУНКЦИЯ 7⁷⁶ of the multiannual financial framework								
Човешки ресурси								
Други административни и разходи		0,240	0,240	0,240	0,240	0,240	0,240	1,20
Междинен сбор извън ФУНКЦИЯ 7 от многогодишната финансова рамка		0,240	0,240	0,240	0,240	0,240	0,240	1,20

ОБЩО		1,770	1,770	1,770	1,770	1,770	1,770	8,850
-------------	--	--------------	--------------	--------------	--------------	--------------	--------------	--------------

Бюджетните кредити, необходими за човешки ресурси и други разходи с административен характер, ще бъдат покрити от бюджетни кредити на ГД, които вече са определени за управлението на действието и/или които са

⁷⁵ Всички цифри в тази колона са ориентировъчни и зависят от продължаването на програмите и наличието на бюджетни кредити.

⁷⁶ Техническа и/или административна помощ и разходи в подкрепа на изпълнението на програми и/или дейности на ЕС (предишни редове ВА), непреки научни изследвания, преки научни изследвания.

преазпределени в рамките на ГД, при необходимост заедно с допълнително отпуснати ресурси, които могат да бъдат предоставени на управляващата ГД в рамките на годишната процедура за отпускане на средства и като се имат предвид бюджетните ограничения.

3.2.3.1. Очаквани нужди от човешки ресурси

- Предложението/инициативата не налага използване на човешки ресурси
- Предложението/инициативата налага използване на човешки ресурси съгласно обяснението по-долу:

Оценката се посочва в еквиваленти на пълно работно време

	Година 2023	Година 2024	Година а 2025	2026	2027	След 2027 г. 77	
•Длъжности в щатното разписание (длъжностни лица и срочно наети служители)							
20 01 02 01 (Централа и представителства на Комисията)	10	10	10	10	10	10	
20 01 02 03 (Делегации)							
01 01 01 01 (Непреки научни изследвания)							
01 01 01 11 (Преки научни изследвания)							
Други бюджетни редове (да се посочат)							
•Външен персонал (в еквивалент на пълно работно време — ЕПРВ)⁷⁸							
20 02 01 (ДНП, КНЕ, ПНА от общия финансов пакет)							
20 02 03 (ДНП, МП, КНЕ, ПНА и МЕД в делегациите)							
XX 01 xx yy zz ⁷⁹	- в централата						
	- в делегациите						
01 01 01 02 (ДНП, КНЕ, ПНА — Непреки научни изследвания)							
01 01 01 12 (ДНП, КНЕ, ПНА — Преки научни изследвания)							
Други бюджетни редове (да се посочат)							
ОБЩО	10	10	10	10	10	10	

XX е съответната област на политиката или бюджетен дял.

Нуждите от човешки ресурси ще бъдат покрити от персонала на ГД, на който вече е възложено управлението на дейността и/или който е преразпределен в рамките на ГД, при необходимост заедно с всички допълнителни отпуснати ресурси, които могат да бъдат предоставени на управляващата ГД в рамките на годишната процедура за отпускане на средства и като се имат предвид бюджетните ограничения.

Очаква се ЕНОЗД да предостави половината от необходимите ресурси.

Описание на задачите, които трябва да се изпълнят:

⁷⁷ Всички цифри в тази колона са ориентировъчни и зависят от продължаването на програмите и наличието на бюджетни кредити.

⁷⁸ ДНП = договорно нает персонал; МП = местен персонал; КНЕ = командирован национален експерт; ПНА = персонал, нает чрез агенции за временна заетост; МЕД = младши експерт в делегация.

⁷⁹ Подтаван за външния персонал, покрит с бюджетните кредити за оперативни разходи (предишни редове ВА).

Длъжностни лица и срочно наети служители	<p>За да се подготвят общо 13—16 заседания, проектодокладите, да се продължи работата по политиката, напр. по отношение на бъдещи изменения на списъка на високорисковите приложения с ИИ, и да се поддържат отношенията с органите на държавите членки ще са необходими 4 AD еквивалента на пълно работно време и 1 AST еквивалент на пълно работно време.</p> <p>За системите с ИИ, разработени от институциите на ЕС, отговаря Европейският надзорен орган по защита на данните. Въз основа на минал опит може да се очаква, че за изпълнението на отговорностите на ЕНОЗД съгласно проекта за законодателен акт са необходими 5 AD еквивалента на пълно работно време.</p>
Външен персонал	

3.2.4. Съвместимост с настоящата многогодишна финансова рамка

Предложението/инициативата:

- може да се финансира изцяло чрез преразпределяне на средства в рамките на съответната функция от многогодишната финансова рамка (МФР).

Не е необходимо препрограмиране.

- налага да се използват неразпределеният марж под съответната функция от МФР и/или специалните инструменти, предвидени в Регламента за МФР.

Обяснете какво е необходимо, като посочите съответните функции, бюджетни редове и суми и инструментите, които се предлага да бъдат използвани.

- налага преразглеждане на МФР.

Обяснете какво е необходимо, като посочите съответните функции, бюджетни редове и суми.

3.2.5. Финансов принос от трети страни

Предложението/инициативата:

- не предвижда съфинансиране от трети страни
- предвижда следното съфинансиране от трети страни, като оценките са дадени по-долу:

Бюджетни кредити в млн. евро (до 3-тия знак след десетичната запетая)

	Година N ⁸⁰	Година N+1	Година N+2	Година N+3	Да се добавят толкова години, колкото е необходимо, за да се обхване продължителността на отражението (вж. точка 1.6)			Общо
Да се посочи съфинансиращият орган								
ОБЩО съфинансирани бюджетни кредити								

⁸⁰

Година N е годината, през която започва да се осъществява предложението/инициативата. Моля, заменете буквата N с очакваната първа година от изпълнението (например: 2021). Същото за следващите години.

3.3. Очаквано отражение върху приходите

- Предложението/инициативата има следното финансово отражение:
- Предложението/инициативата има следното финансово отражение:
 - върху разните приходи
 - върху разните приходи
 - Моля, посочете дали приходите са записани по разходни бюджетни редове

млн. евро (до 3-тия знак след десетичната запетая)

Приходен ред:	бюджетен	Налични бюджетни кредити за текущата финансова година	Отражение на предложението/инициативата ⁸¹				Да се добавят толкова години, колкото е необходимо, за да се обхване продължителността на отражението (вж. точка 1.6)	
			Година N	Година N+1	Година N+2	Година N+3		
Статия								

За целевите приходи да се посочат съответните разходни бюджетни редове.

--

Други забележки (например метод/формула за изчисляване на отражението върху приходите или друга информация).

--

⁸¹

Що се отнася до традиционните собствени ресурси (мита, налози върху захарта), посочените суми трябва да бъдат нетни, т.е. брутни суми, от които са приспаднали 20 % за разходи по събирането.