



2024/1689

12.7.2024 г.

РЕГЛАМЕНТ (ЕС) 2024/1689 НА ЕВРОПЕЙСКИЯ ПАРЛАМЕНТ И НА СЪВЕТА

от 13 юни 2024 година

за установяване на хармонизирани правила относно изкуствения интелект и за изменение на регламенти (ЕО) № 300/2008, (ЕО) № 167/2013, (ЕО) № 168/2013, (ЕО) 2018/858, (ЕО) 2018/1139 и (ЕО) 2019/2144 и директиви 2014/90/ЕС, (ЕО) 2016/797 и (ЕО) 2020/1828 (Акт за изкуствения интелект)

(текст от значение за ЕИП)

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 комитет ⁽¹⁾,

като взеха предвид становището на Европейската централна банка ⁽²⁾,

като взеха предвид становището на Комитета на регионите ⁽³⁾,

в съответствие с обикновената законодателна процедура ⁽⁴⁾,

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, пускането на пазара, пускането в действие и използването на системи с изкуствен интелект (наричани по-долу „системи с ИИ“) в Съюза, в съответствие с ценностите на Съюза, да се насърчи навлизането на ориентиран към човека и надежден изкуствен интелект (ИИ), като същевременно се гарантира високо равнище на защита на здравето, безопасността и основните права, залегнали в Хартата на основните права на Европейския съюз (наричана по-долу „Хартата“), включително демокрацията, принципите на правовата държава и опазването на околната среда, да се осигури защита срещу вредните последици от системите с ИИ в Съюза и да се подкрепят иновациите. С настоящия регламент се гарантира свободното трансгранично движение на стоки и услуги, основани 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 не е изрично разрешено с настоящия регламент.
- (2) Настоящият регламент следва да се прилага в съответствие с ценностите на Съюза, залегнали в Хартата, като се улеснява защитата на физическите лица, предприятията, демокрацията, принципите на правовата държава и опазването на околната среда и същевременно се насърчават иновациите и заетостта и се спомага за превръщането на Съюза в лидер във възприемането на надежден ИИ.
- (3) Системите с ИИ могат лесно да бъдат внедрени в най-различни сектори на икономиката и в много 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 ИИ е надежден и безопасен и се разработва и използва в съответствие със задълженията, свързани с основните права. Различаващите се национални правила могат да доведат до разпокъсаност на вътрешния пазар и да намалят правната сигурност за операторите, които разработват, внасят или използват системи с ИИ. Ето защо, с цел да се осигури надежден ИИ, следва да се гарантира последователно и високо равнище на защита в целия Съюз, като същевременно се предотвратят различията, възпрепятстващи свободното движение, иновациите, внедряването и възприемането в рамките на

⁽¹⁾ ОВ С 517, 22.12.2021 г., стр. 56.

⁽²⁾ ОВ С 115, 11.3.2022 г., стр. 5.

⁽³⁾ ОВ С 97, 28.2.2022 г., стр. 60.

⁽⁴⁾ Позиция на Европейския парламент от 13 март 2024 г. (все още непубликувана в Официален вестник) и решение на Съвета от 21 май 2024 г.

вътрешния пазар на системи с ИИ и свързани с тях продукти и услуги, като за целта се предвидят еднакви задължения за операторите и се гарантира еднаква защита на императивните съображения от обществен интерес и на правата на лицата в рамките 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 за правоохранителни цели, за използването на системи с ИИ за оценка на риска за физическите лица за правоохранителни цели и за използването на системи с ИИ за биометрично категоризиране за правоохранителни цели, е целесъобразно правното основание на настоящия регламент, във връзка с тези специални правила, да бъде член 16 ДФЕС. С оглед на тези специални правила и защитата съгласно член 16 ДФЕС е целесъобразно да се проведе консултация с Европейския комитет по защита на данните.

- (4) ИИ е бързо развиваща се съвкупност от технологии, които допринасят за извличането на множество икономически, екологични и обществени ползи по протежение на целия спектър от стопански сектори и социални дейности. Като подобрява прогнозирането, оптимизира операциите и разпределянето на ресурсите и персонализира цифровите решения, които са на разположение на физическите лица и организациите, използването на ИИ може да осигури ключови конкурентни предимства за предприятията и да спомогне за постигането на социално и екологично благоприятни резултати, например в областта на здравеопазването, селското стопанство, безопасността на храните, образованието и обучението, медиите, спорта, културата, управлението на инфраструктурата, енергетиката, транспорта и логистиката, публичните услуги, сигурността, правосъдието, ресурсната и енергийната ефективност, мониторинга на околната среда, опазването и възстановяването на биоразнообразието и екосистемите, както и смекчаването на последиците от изменението на климата и адаптирането към него.
- (5) Същевременно, в зависимост от обстоятелствата по отношение на конкретното му приложение, използване и равнище на технологично развитие, ИИ може да доведе до рискове и да накърни обществените интереси и основните права, защитени от правото на Съюза. Тези вреди могат да бъдат имуществени или неимуществени, включително физически, психически, обществени или икономически.
- (6) Предвид значителното въздействие, което ИИ може да окаже върху обществото, и необходимостта от изграждане на доверие, е от жизненоважно значение ИИ и неговата регулаторна рамка да бъдат разработени в съответствие с ценностите на Съюза, залегнали в член 2 от Договора за Европейския съюз (ДЕС), и основните права и свободи, залегнали в Договорите и, съгласно член 6 ДЕС, в Хартата. Като предварително условие ИИ следва да бъде технология, ориентирана към човека. Той следва да служи като инструмент за хората, като крайната цел е да се повиши тяхното благосъстояние.
- (7) За да се гарантира последователно и високо равнище на защита на обществените интереси по отношение на здравето, безопасността и основните права, следва да бъдат установени общи правила за високорисковите системи с ИИ. Тези правила следва да бъдат в съответствие с Хартата, да бъдат недискриминационни и да са в съответствие с международните търговски ангажменти на Съюза. Освен това те следва да са съобразени с Европейската декларация относно цифровите права и принципи за цифровото десетилетие и Насоките относно етичните аспекти за надежден ИИ на експертната група на високо равнище по въпросите на изкуствения интелект (ЕГВР ИИ).
- (8) Поради това е необходима правна рамка на Съюза, с която да се установят хармонизирани правила относно ИИ, за да се насърчи разработването, използването и навлизането на ИИ на вътрешния пазар, и която същевременно да осигурява високо равнище на защита на обществените интереси, например здравето и безопасността, и защитата на основните права, включително демокрацията, принципите на правовата държава и опазването на околната среда, признати и защитени от правото на Съюза. За постигането на тази цел следва да бъдат установени правила, уреждащи пускането на пазара, пускането в действие и използването 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. Тези правила следва да бъдат ясни и надеждни по отношение на защитата на основните права, да благоприятстват нови иновативни решения и да дават възможност за изграждане на европейска екосистема от публични и частни участници, които да създават системи с ИИ в съответствие с ценностите на Съюза и да отключват потенциала на цифровата трансформация във всички региони на Съюза. С установяването на такива правила, както и на мерки в подкрепа на иновациите с отделяне на специално внимание на малките и средните предприятия (МСП), включително новосъздадените предприятия, настоящият регламент подкрепя целта за насърчаване на европейския подход към ИИ, ориентиран към човека, и целта на Съюза да бъде световен лидер в разработването на сигурен, надежден и етичен ИИ, както бе посочено от Европейския съвет⁽⁵⁾, и гарантира защитата на етичните принципи, както изрично бе поискано от Европейския парламент⁽⁶⁾.

⁽⁵⁾ Европейски съвет, извънредно заседание на Европейския съвет (1 и 2 октомври 2020 г.) – Закljučения, EUCO 13/20, 2020 г., стр. 6.

⁽⁶⁾ 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).

- (9) Следва да бъдат установени хармонизирани правила, приложими за пускането на пазара, пускането в действие и използването на високорискови системи с ИИ, в съответствие с Регламент (ЕО) № 765/2008 на Европейския парламент и на Съвета⁽⁷⁾, Решение № 768/2008/ЕО на Европейския парламент и на Съвета⁽⁸⁾ и Регламент (ЕС) 2019/1020 на Европейския парламент и на Съвета⁽⁹⁾ (наричани по-долу „новата законодателна рамка“). Хармонизираните правила, установени в настоящия регламент, следва да се прилагат във всички сектори и, в съответствие с новата законодателна рамка, следва да не засягат действащото право на Съюза, по-специално в областта на защитата на данните, защитата на потребителите, основните права, заетостта, защитата на работниците и безопасността на продуктите, което настоящият регламент допълва. В резултат на това всички права и правни средства за защита, предвидени в това право на Съюза в интерес на потребителите и други лица, върху които системите с ИИ могат да оказват отрицателно въздействие, включително по отношение на обезщетението за евентуални вреди съгласно Директива 85/374/ЕИО на Съвета⁽¹⁰⁾, остават незасегнати и напълно приложими. Наред с това, в контекста на заетостта и защитата на работниците, настоящият регламент не следва да засяга правото на Съюза в областта на социалната политика и националното трудово право, което е в съответствие с правото на Съюза, относно условията на заетост и труд, включително здравословните и безопасни условия на труд и отношенията между работодателите и работниците. Настоящият регламент не следва да засяга и упражняването на основни права, признати в държавите членки и на равнището на Съюза, включително правото или свободата на стачка или на други действия, обхванати от специалните системи на колективни трудови правоотношения в държавите членки, както и правото да се преговаря, да се сключват и прилагат колективни трудови договори или да се предприемат колективни действия в съответствие с националното право. Настоящият регламент не следва да засяга разпоредбите, насочени към подобряване на условията на труд при работа през платформа, предвидени в директива на Европейския парламент и на Съвета относно подобряването на условията на труд при работата през платформа. Освен това настоящият регламент има за цел да повиши ефективността на тези съществуващи права и правни средства за защита чрез установяване на конкретни изисквания и задължения, включително по отношение на прозрачността, техническата документация и поддържането на регистри по отношение на системите с ИИ. Наред с това задълженията, наложени на различните оператори, участващи във веригата за създаване на стойност в областта на ИИ съгласно настоящия регламент, следва да се прилагат, без да се засяга националното право, съвместимо с правото на Съюза и което води до ограничаване на използването на определени системи с ИИ, когато това право е извън приложното поле на настоящия регламент или преследва законни цели от обществен интерес, различни от преследваните с настоящия регламент. Например националното трудово право и правото за закрила на ненавършилият пълнолетие лица, а именно лицата на възраст под 18 години, като се вземе предвид Общ коментар № 25 (2021) на Комитета по правата на детето на Организацията на обединените нации относно правата на децата във връзка с цифровата среда, доколкото те не са конкретно насочени към системите с ИИ и преследват други законни цели от обществен интерес, не следва да бъдат засегнати от настоящия регламент.
- (10) Основното право на защита на личните данни е гарантирано по-специално с регламенти (ЕС) 2016/679⁽¹¹⁾ и (ЕС) 2018/1725⁽¹²⁾ на Европейския парламент и на Съвета и с Директива (ЕС) 2016/680 на Европейския парламент и на Съвета⁽¹³⁾. Директива 2002/58/ЕО на Европейския парламент и на Съвета⁽¹⁴⁾ допълнително защитава личния живот и поверителността на съобщенията, включително чрез установяване на условията за съхраняване на лични и нелични данни в крайно оборудване и достъп до такива данни от крайно оборудване. Посочените правни актове на Съюза осигуряват основата за устойчиво и отговорно обработване на данни, включително когато наборите от данни включват комбинация от лични и нелични данни. Настоящият регламент няма за цел да засегне прилагането на съществуващото право на Съюза, уреждащо обработването на лични данни, включително задачите и правомощията на независимите надзорни органи, компетентни да наблюдават спазването на тези инструменти. Освен това той не засяга задълженията на доставчиците и внедрителите на системи с ИИ в ролята им на администратори или обработващи лични данни, които произтичат от правото на Съюза или националното право относно защитата на личните данни, доколкото проектирането, разработването или използването на системи с ИИ включва обработването на лични данни.
- (7) Регламент (ЕО) № 765/2008 на Европейския парламент и на Съвета от 9 юли 2008 г. за определяне на изискванията за акредитация и за отмяна на Регламент (ЕИО) № 339/93 (ОВ L 218, 13.8.2008 г., стр. 30).
- (8) 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).
- (9) 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 (ОВ L 169, 25.6.2019 г., стр. 1).
- (10) Директива 85/374/ЕИО на Съвета от 25 юли 1985 г. за сближаване на законовите, подзаконовите и административните разпоредби на държавите членки относно отговорността за вреди, причинени от дефект на стока (ОВ L 210, 7.8.1985 г., стр. 29).
- (11) 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).
- (12) 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).
- (13) 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 (ОВ L 119, 4.5.2016 г., стр. 89).
- (14) Директива 2002/58/ЕО на Европейския парламент и на Съвета от 12 юли 2002 г. относно обработката на лични данни и защита на правото на неприкосновеност на личния живот в сектора на електронните комуникации (Директива за правото на неприкосновеност на личния живот и електронни комуникации) (ОВ L 201, 31.7.2002 г., стр. 37).

Целесъобразно е също така да се поясни, че субектите на данни продължават да се ползват с всички права и гаранции, предоставени им с посоченото право на Съюза, включително правата, свързани с изцяло автоматизираното вземане на индивидуални решения, включително профилирането. Хармонизираните правила относно пускането на пазара, пускането в действие и използването на системи с ИИ, установени съгласно настоящия регламент, следва да улеснят ефективното прилагане и да позволят упражняването на правата на субектите на данни и другите правни средства за защита, гарантирани с правото на Съюза в областта на защитата на личните данни, и на други основни права.

- (11) Настоящият регламент следва да не засяга разпоредбите относно отговорността на доставчиците на посреднически услуги, установени в Регламент (ЕС) 2022/2065 на Европейския парламент и на Съвета ⁽¹⁵⁾.
- (12) Понятието „система с ИИ“ в настоящия регламент следва да бъде ясно определено и тясно съгласувано с резултатите от работата на международни организации в областта на ИИ, за да се гарантира правна сигурност и да се улесни сближаването и широкото приемане в международен план, като същевременно се осигури гъвкавост с цел да се реагира на бързото технологично развитие в тази област. Освен това определението следва да се основава на ключови характеристики на системите с ИИ, които ги отличават от по-прости традиционни софтуерни системи или подходи за програмиране, и не следва да обхваща системи, които се основават на правилата, определени единствено от физически лица за автоматично изпълнение на операциите. Ключова характеристика на системите с ИИ е тяхната способност да правят изводи. Тази способност да се правят изводи се отнася до процеса на получаване на резултати, например прогнози, съдържание, препоръки или решения, които могат да повлияят на физическата и виртуалната среда, както и до способността на системите с ИИ да извличат модели или алгоритми, или и двете, от входяща информация или данни. Техниките, даващи възможност да се правят изводи при изграждането на системи с ИИ, включват подходи за машинно обучение, при които те се учат от данните как да постигнат определени цели, както и основани на логика и знания подходи, при които достигат до изводи от кодирани знания или символично представяне на задачата, която трябва да бъде решена. Способността на дадена система с ИИ да прави изводи надхвърля основната обработка на данни, като дава възможност за обучение, разсъждение или моделиране. Понятието „машинно базиран“ се отнася до факта, че системите с ИИ работят с помощта на машини. С позоваването на явни или подразбиращи цели се подчертава, че системите с ИИ могат да работят в съответствие с ясно определени или с подразбиращи се цели. Целите на дадена система с ИИ може да се различават от предназначението на системата с ИИ в специфичен контекст. За целите на настоящия регламент под „среда“ следва да се разбира контекстът, в който функционират системите с ИИ, а резултатите, генерирани от системата с ИИ, отразяват различни функции, изпълнявани от системите с ИИ, и включват прогнози, съдържание, препоръки или решения. Системите с ИИ са проектирани да функционират с различна степен на автономност, което означава, че те разполагат с известна степен на независимост на действията от участието на човека и на способност за работа без човешка намеса. Адаптивността, която дадена система с ИИ би могла да прояви след внедряването ѝ, се отнася до способностите за самообучение, които позволяват на системата да се променя по време на нейното използване. Системите с ИИ могат 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).
- (13) Понятието „внедрител“, посочено в настоящия регламент, следва да се тълкува като всяко физическо или юридическо лице, включително публичен орган, агенция или друга структура, които използват система с ИИ, върху която упражняват контрол, с изключение на случаите, когато системата с ИИ се използва в процеса на лична непрофесионална дейност. В зависимост от вида на системата с ИИ използването на системата може да засегне лица, различни от внедрителя.
- (14) Понятието „биометрични данни“, посочено в настоящия регламент, следва да се тълкува с оглед на понятието за биометрични данни съгласно определението в член 4, точка 14 от Регламент (ЕС) 2016/679, член 3, точка 18 от Регламент (ЕС) 2018/1725 и член 3, точка 13 от Директива (ЕС) 2016/680. Биометричните данни могат да позволят удостоверяване на самоличността, идентифициране или категоризиране на физически лица, както и разпознаване на емоции на физически лица.
- (15) Понятието „биометрична идентификация“, посочено в настоящия регламент, следва да се определи като автоматизираното разпознаване на физически, физиологични и поведенчески характеристики на човека, например лице, движение на очите, форма на тялото, глас, ритъм и интонация на говора, походка, стойка, сърдечен ритъм, кръвно налягане, мирис и особености на натиска на клавиши, с цел установяване на самоличността на дадено лице чрез сравняване на биометрични данни на това лице със съхранени биометрични данни на лица в референтна база данни, независимо дали лицето е дало своето съгласие. Това изключва системите с ИИ, предназначени да бъдат използвани за биометрична проверка, която включва удостоверяване на самоличността, чиято единствена цел е да се потвърди, че конкретно физическо лице е лицето, за което се представя, и да се потвърди самоличността на физическо лице единствено за да се получи достъп до услуга, да се отключи устройство или да се придобие сигурен достъп до помещения.

⁽¹⁵⁾ Регламент (ЕС) 2022/2065 на Европейския парламент и на Съвета от 19 октомври 2022 г. относно единния пазар на цифрови услуги и за изменение на Директива 2000/31/ЕО (Акт за цифровите услуги) (ОВ L 277, 27.10.2022 г., стр. 1).

- (16) Понятието „биометрично категоризиране“, посочено в настоящия регламент, следва да се определи като отнасяне на физически лица към конкретни категории въз основа на техните биометрични данни. Подобни конкретни категории могат да са свързани с аспекти като пол, възраст, цвят на косата, цвят на очите, татуировки, поведенчески или личностни черти, език, религия, принадлежност към национално малцинство, сексуална или политическа ориентация. Това не включва системи за биометрично категоризиране, които представляват чисто спомагателна функция, неразривно свързана с друга търговска услуга, което означава, че тази функция не може по обективни технически причини да се използва без основната услуга и интегрирането на тази функция или функционалност не е средство за заобикаляне на приложимостта на правилата на настоящия регламент. Например филтрите за категоризиране на черти на лицето или тялото, използвани на онлайн места за търговия, биха могли да представляват такава спомагателна функция, тъй като могат да се използват само във връзка с основната услуга, която се състои в продажбата на продукт, като позволяват на потребителя да визуализира изображението на продукта върху себе си и му помагат да вземе решение при покупка. Филтрите, използвани в онлайн услугите на социалните мрежи, които категоризират черти на лицето или тялото, за да позволят на ползвателите да добавят или променят снимки или видеоклипове, също могат да се считат за спомагателна функция, тъй като такъв филтър не може да се използва без основната услуга при услугите на социалните мрежи, състояща се в споделяне на съдържание онлайн.
- (17) Понятието „система за дистанционна биометрична идентификация“, посочено в настоящия регламент, следва да се определи функционално като система с ИИ, предназначена за идентифициране на физически лица без тяхното активно участие, обикновено от разстояние, чрез сравняване на биометричните данни на дадено лице с биометричните данни, съдържащи се в референтна база данни, независимо от конкретните използвани технологии, процеси или видове биометрични данни. Такива системи за дистанционна биометрична идентификация обикновено се използват за едновременно наблюдение на множество лица или тяхното поведение с цел да се улесни значително идентифицирането на физически лица без тяхното активно участие. Това изключва системите с ИИ, предназначени да бъдат използвани за биометрична проверка, която включва удостоверяване на самоличността, чиято единствена цел е да се потвърди, че конкретно физическо лице е лицето, за което се представя, и да се потвърди самоличността на физическо лице единствено за да се получи достъп до услуга, да се отключи устройство или да се придобие сигурен достъп до помещения. Това изключване е обосновано от факта, че е вероятно такива системи да оказват незначително въздействие върху основните права на физическите лица в сравнение със системите за дистанционна биометрична идентификация, които могат да се използват за обработването на биометрични данни на голям брой лица без тяхното активно участие. 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 съответните 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 функциониращите впоследствие системи 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 съответните физически лица.
- (18) Понятието „система за разпознаване на емоции“, посочено в настоящия регламент, следва да се определи като система с ИИ, чието предназначение е да определи или да прави изводи за емоциите или намеренията на физически лица въз основа на техните биометрични данни. Това понятие се отнася до емоции или намерения като щастие, тъга, гняв, изненада, отвращение, смущение, вълнение, срам, презрение, удовлетворение и забавление. Не се включват физически състояния като болка или умора, като например системи, използвани за установяване на състояние на умора при професионални пилоти или водачи с цел предотвратяване на произшествия. Освен това то не включва откриването на лесно забележими изражения, жестове или движения, освен ако те не се използват, за да се определят или да се правят изводи за емоциите. Тези изражения могат да бъдат основни изражения на лицето, като например намръщване или усмивка, или жестове като движение на ръцете или главата, или характеристики на човешкия глас, например висок глас или шепот.
- (19) За целите на настоящия регламент понятието „обществено достъпно място“ следва да се разбира като означаващо всяко физическо място, което е достъпно за неопределен брой физически лица, независимо дали това място е частна или публична собственост и без значение от дейността, за която мястото може да се използва, като за търговия, например магазини, ресторанти, кафенета, за услуги, например банки, професионални дейности, хотелиерство и ресторантьорство, за спорт, например плувни басейни, спортни зали, стадиони, за транспорт, например автобусни, метро и железопътни гари, летища, транспортни средства, за развлечение, например кина, театри, музеи, концертни и конферентни зали, за отход или други дейности, например отворени за обществено ползване пътища, площи, паркове, гори, детски площадки. Дадено място следва също така да се класифицира като обществено достъпно ако, независимо от потенциалния капацитет или ограниченията във връзка със сигурността, достъпът до него зависи от някои предварително определени условия, които могат да бъдат изпълнени от неопределен брой лица, като например закупуване на билет или друг превозен документ, предварителна регистрация или навършване на определена възраст. Дадено място не следва обаче да се счита за обществено достъпно, ако достъпът до него е ограничен до конкретни и определени физически лица чрез правото на Съюза или националното право, пряко свързано с обществената безопасност или сигурност, или чрез ясното волеизявление от страна на лицето, което е носител на съответните права

по отношение на мястото. Единствено фактическата възможност за достъп, например незаклучена врата или отворена порта в ограда, не означава, че мястото е обществено достъпно, при наличие на признаци или обстоятелства, които предполагат обратното, например знаци, забраняващи или ограничаващи достъпа. Помещенията на дадено дружество и фабрика, както и офисите и работните места, до които се предвижда достъп само за съответните служители и доставчици на услуги, не са обществено достъпни места. Обществено достъпните места не следва да включват затворите или зоните за граничен контрол. Други зони могат да се състоят както от зони, които са обществено достъпни, така и от зони, които не са обществено достъпни, като например коридорите в частни жилищни сгради, необходими за достъп до лекарски кабинет, или летищата. Онлайн пространствата не се включват, тъй като те не са физически места. Дали дадено място е достъпно за обществеността обаче следва да се определя отделно във всеки един случай, като се отчитат особеностите на отделния случай.

- (20) За да се извлекат максимални ползи от системите с ИИ, като същевременно се защитават основните права, здравето и безопасността, и за да се даде възможност за демократичен контрол, грамотността в областта на ИИ следва да осигури на доставчиците, внедрителите и засегнатите лица необходимите понятия за вземане на информирани решения относно системите с ИИ. Тези понятия могат да се различават по отношение на съответния контекст и могат да включват разбиране на правилното прилагане на техническите елементи по време на етапа на разработване на системата с ИИ, мерките, които трябва да се прилагат по време на използването ѝ, подходящите начини за тълкуване на резултатите от системата с ИИ и, по отношение на засегнатите лица, знанията, необходими за разбиране на начина, по който решенията, взети с помощта на ИИ, ще окажат въздействие върху тях. В контекста на прилагането на настоящия регламент грамотността в областта на ИИ следва да осигури на всички съответни участници във веригата за създаване на стойност в областта на ИИ необходимата информация, за да се гарантира подходящото спазване и правилното му прилагане. Освен това широкото прилагане на мерки за повишаване на грамотността в областта на ИИ и въвеждането на подходящи последващи действия биха могли да допринесат за подобряване на условията на труд и в крайна сметка да поддържат процеса на утвърждаване и иновации на надеждния ИИ в Съюза. Европейският съвет по изкуствен интелект (наричан по-долу „Съветът по ИИ“) следва да подпомага Комисията с цел насърчаване на инструментите за грамотност в областта на ИИ, обществената осведоменост и разбирането на ползите, рисковете, гаранциите, правата и задълженията във връзка с използването на системи с ИИ. В сътрудничество със съответните заинтересовани страни Комисията и държавите членки следва да улеснят изготвянето на незадължителни кодекси за поведение с цел повишаване на грамотността в областта на ИИ сред лицата, занимаващи се с разработването, експлоатацията и използването на ИИ.
- (21) За да се гарантират равнопоставеност и ефективна защита на правата и свободите на физическите лица в целия Съюз, правилата, установени с настоящия регламент, следва да се прилагат недискриминационно за доставчиците на системи с ИИ, независимо дали са установени в Съюза, или в трета държава, както и за внедрителите на системи с ИИ, установени в Съюза.
- (22) 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 пускат в действие и не се използват в Съюза. Такъв е например случаят с оператор, установен в Съюза, който сключва договор за определени услуги с оператор, установен в трета държава, във връзка с дейност, която ще се извършва от система с ИИ, която би била определена като високорискова. При тези обстоятелства системата с ИИ, използвана в трета държава от оператора, би могла да обработва данни, които са законно събрани в Съюза и прехвърлени от Съюза, и да предоставя на сключилия договор оператор в Съюза резултата от системата с ИИ, получен въз основа на тази обработка, без системата с ИИ да е била пускана на пазара, пусната в действие 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 внедрителите на системи с ИИ, установени в трета държава, доколкото резултатът, получен от тези системи, е предназначен да се използва в Съюза. Независимо от това, за да се вземат предвид съществуващите договорености и особените нужди от бъдещо сътрудничество с чуждестранни партньори, с които се обменят информация и доказателства, настоящият регламент не следва да се прилага за публични органи на трета държава и за международни организации, когато те действат в рамките на споразумения за сътрудничество или международни споразумения, сключени на равнището на Съюза или на национално равнище за сътрудничество в областта на правоприлагането и за съдебно сътрудничество със Съюза или с неговите държави членки, при условие че съответната трета държава или международна организация осигурява подходящи гаранции по отношение на защитата на основните права и свободи на лицата. Когато е приложимо, това може да обхваща дейности на субекти, на които третите държави са възложили изпълнението на конкретни задачи в подкрепа на това сътрудничество в областта на правоприлагането и съдебно сътрудничество. Такива рамки за сътрудничество или споразумения са установени двустранно между държави членки и трети държави или между Европейския съюз, Европол и други агенции на Съюза, трети държави и международни организации. Органите, компетентни за надзора на правоохранителните органи и органите на съдебната власт съгласно настоящия регламент, следва да преценят дали тези рамки за сътрудничество или международни споразумения включват подходящи гаранции по отношение на защитата на основните права и свободи на лицата. Националните органи и институциите, органите, службите и агенциите на

Съюза, които получават и използват такива резултати в Съюза, продължават да са задължени да гарантират, че използването им е в съответствие с правото на Съюза. Когато тези международни споразумения се преразглеждат или се сключват нови в бъдеще, договарящите страни следва да положат максимални усилия да приведат тези споразумения в съответствие с изискванията на настоящия регламент.

- (23) Настоящият регламент следва да се прилага и за институциите, органите, службите и агенциите на Съюза, когато те действат като доставчик или внедрител на система с ИИ.
- (24) Ако и доколкото системите с ИИ се пускат на пазара, пускат в действие или използват, със или без изменение на тези системи, за военни цели и цели, свързани с отбраната или националната сигурност, те следва да бъдат изключени от обхвата на настоящия регламент, независимо от това какъв вид субект извършва тези дейности, например дали е публичен, или частен субект. По отношение на военните цели и целите, свързани с отбраната, това изключение е обосновано както от член 4, параграф 2 ДЕС, така и от специфичните особености на политиката за отбрана на държавите членки и общата политика за отбрана на Съюза, обхваната от дял V, глава 2 ДЕС, спрямо които се прилага международното публично право, което поради това е по-подходящата правна рамка за регулиране на системите с ИИ в контекста на употребата на смъртоносна сила и на други системи с ИИ в контекста на военните и отбранителните дейности. По отношение на целите на националната сигурност, изключението е обосновано както от факта, че националната сигурност продължава да бъде отговорност единствено на държавите членки в съответствие с член 4, параграф 2 ДЕС, така и от специфичното естество и оперативни нужди на дейностите в областта на националната сигурност и специалните национални правила, приложими за тези дейности. Въпреки това, ако система с ИИ, разработена, пусната на пазара, пусната в действие или използвана за военни цели и цели, свързани с отбраната или националната сигурност, се използва извън рамките на тези цели временно или се използва постоянно за други цели, например за граждански или хуманитарни цели и за правоохранителни цели или цели, свързани с обществената сигурност, тази система би попаднала в обхвата на настоящия регламент. В този случай субектът, използващ системата с ИИ за цели, различни от военни цели и цели, свързани с отбраната или националната сигурност, следва да гарантира съответствието на системата с ИИ с настоящия регламент, освен ако системата вече не е в съответствие с настоящия регламент. Системите с ИИ, пуснати на пазара или пуснати в действие за изключена цел, а именно военна цел и цел, свързана с отбраната или национална сигурност, и една или повече неизключени цели, например граждански цели или правоохранителни цели, попадат в обхвата на настоящия регламент и доставчиците на тези системи следва да гарантират спазването на настоящия регламент. В тези случаи фактът, че дадена система с ИИ може да попадне в обхвата на настоящия регламент, не следва да засяга възможността субектите, извършващи дейности в областта на националната сигурност и отбраната и военни дейности, независимо от вида на субекта, извършващ тези дейности, да използват за цели в областта на националната сигурност и отбраната и за военни цели системи с ИИ, чието използване е изключено от обхвата на настоящия регламент. Система с ИИ, пусната на пазара за граждански цели или за правоохранителни цели, която се използва, със или без изменение, за военни цели и за цели, свързани с отбраната или националната сигурност, не следва да попада в обхвата на настоящия регламент, независимо от вида на субекта, извършващ тези дейности.
- (25) Настоящият регламент следва да подкрепя иновациите, да защита свободата на науката и не следва да е пречка за научноизследователската и развойната дейност. Поради това е необходимо от неговия обхват да бъдат изключени системите и моделите с ИИ, специално разработени и пуснати в действие единствено с цел научноизследователска и развойна дейност. Освен това е необходимо да се гарантира, че настоящият регламент не засяга по друг начин научноизследователската и развойната дейност в областта на системите или моделите с ИИ преди пускането им на пазара или пускането им в действие. По отношение на ориентираната към продуктите научноизследователска, изпитателна и развойна дейност във връзка със системи или модели с ИИ, разпоредбите на настоящия регламент също така не следва да се прилагат преди пускането в действие или пускането на пазара на тези системи и модели. Това изключение не засяга задължението за спазване на настоящия регламент, когато система с ИИ, попадаща в обхвата на настоящия регламент, е пусната на пазара или пусната в действие в резултат на такава научноизследователска и развойна дейност, както и прилагането на разпоредбите относно регулаторните лаборатории в областта на ИИ и изпитването в реални условия. Освен това, без да се засяга изключението по отношение на системите с ИИ, специално разработени и пуснати в действие единствено за целите на научноизследователската и развойната дейност, за всяка друга система с ИИ, която може да се използва за извършването на научноизследователска и развойна дейност, разпоредбите на настоящия регламент следва да продължат да се прилагат. Във всеки случай всяка научноизследователска и развойна дейност следва да се извършва в съответствие с признатите етични и професионални стандарти по отношение на научните изследвания и следва да се провежда в съответствие с приложимото право на Съюза.
- (26) 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 обхвата на рисковете, които системите с ИИ могат да породят. Поради това е необходимо да се забранят някои неприемливи практики в областта на ИИ, да се установят изисквания за високорисковите системи с ИИ и задължения за съответните оператори, както и да се установят задължения за прозрачност за някои системи с ИИ.

- (27) Въпреки че основаният на риска подход е основата за пропорционален и ефективен набор от задължителни правила, е важно да се припомнят Насоките относно етичните аспекти за надежден ИИ от 2019 г., разработени от независимата ЕГВР ИИ, определена от Комисията. В тези насоки ЕГВР ИИ е разработила седем необвързващи етични принципа за ИИ, които имат за цел да спомогнат да се гарантира, че ИИ е надежден и етичен. Седемте принципа включват човешки фактор и контрол; техническа стабилност и безопасност; неприкосновеност на личния живот и управление на данните; прозрачност; многообразие, недискриминация и справедливост; обществено и екологично благосъстояние; отчетност. Без да засягат правно обвързващите изисквания на настоящия регламент и на всички други приложими правни актове на Съюза, посочените насоки допринасят за разработването на съгласуван, надежден и ориентиран към човека ИИ в съответствие с Хартата и с ценностите, на които се основава Съюзът. Съгласно Насоките на ЕГВР ИИ човешки фактор и контрол означава, че системите с ИИ се разработват и използват като инструмент, който служи на хората, защита човешкото достойнство и личната независимост и функционира така, че да може да се контролира и наблюдава от хората по подходящ начин. Техническа стабилност и безопасност означава, че системите с ИИ се разработват и използват по начин, който позволява стабилност в случай на проблеми и устойчивост срещу опити за промяна на използването или действието на системата с ИИ, така че да се даде възможност за незаконно използване от трети лица, и който свежда до минимум непреднамерените вреди. Неприкосновеност на личния живот и управление на данните означава, че системите с ИИ се разработват и използват в съответствие с правилата относно неприкосновеността на личния живот и защитата на данните, като същевременно се обработват данни, които отговарят на високи стандарти по отношение на качеството и целостта. Прозрачност означава, че системите с ИИ се разработват и използват по начин, който позволява подходяща проследимост и разбираемост, като същевременно хората се уведомяват, че комуникират или си взаимодействат със система с ИИ, и внедрителите надлежно се информират за способностите и ограниченията на тази система с ИИ, а засегнатите лица – за техните права. Многообразие, недискриминация и справедливост означава, че системите с ИИ се разработват и използват по начин, който включва различни участници и насърчава равния достъп, равенството между половете и културното многообразие, като същевременно се избягват дискриминационните въздействия и несправедливата предубеденост, които са забранени от правото на Съюза или националното право. Обществено и екологично благосъстояние означава, че системите с ИИ се разработват и използват по устойчив и екологосъобразен начин, както и така, че да са от полза за всички хора, като същевременно се наблюдават и оценяват дългосрочните въздействия върху отделните лица, обществото и демокрацията. Прилагането на тези принципи следва да бъде отразено, когато е възможно, при проектирането и използването на модели с ИИ. При всички случаи те следва да служат като основа за изготвянето на кодекси за поведение съгласно настоящия регламент. Всички заинтересовани страни, включително стопанските сектори, академичните среди, гражданското общество и организациите за стандартизация, се насърчават да вземат предвид, когато е целесъобразно, етичните принципи за разработването на незадължителни най-добри практики и стандарти.
- (28) Въпреки че ИИ има многобройни полезни приложения, с него може да се злоупотребява и той може да осигури нови и мощни инструменти за манипулативни и експлоататорски практики и практики за социален контрол. Тези практики са особено вредни и недоброръководни 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 основните права, залегнали в Хартата, включително правото на недискриминация, на защита на данните и на неприкосновеност на личния живот, както и правата на детето.
- (29) Манипулативните техники, използващи ИИ, могат да служат за склоняване на хората към нежелано поведение или за подвеждането им, като ги подтиква да вземат решения по начин, който подкопава и накрънява тяхната независимост, вземане на решения и свободен избор. Пускането на пазара, пускането в действие или използването на някои системи с ИИ с цел или последици, изразяващи се в съществено изменение на човешкото поведение, при което е вероятно да възникнат значителни вреди, по-специално оказващи достатъчно значимо неблагоприятно въздействие върху физическото или психологическото здраве или финансовите интереси, са особено опасни и поради това следва да бъдат забранени. Такива системи с ИИ използват компоненти, действащи на подсъзнанието, например стимули чрез изображения и аудио и видео стимули, които хората не могат да възприемат, тъй като тези стимули са отвъд човешкото възприятие, или други манипулативни или заблуждаващи техники, които подкопават или накръняват независимостта, вземането на решения или свободния избор така, че хората не осъзнават, че се използват такива техники, или дори когато го осъзнават, те все пак могат да бъдат заблудени или не са в състояние да ги контролират или да им устоят. Това може да бъде улеснено например от интерфейси мозък-машина или виртуална реалност, тъй като те позволяват по-висока степен на контрол върху това какви стимули се предоставят на хората, доколкото те могат съществено да променят поведението им по начин, който води до значителна вреда. Наред с това системите с ИИ могат да се възползват и по друг начин от уязвимостта на дадено лице или конкретна група лица поради тяхната възраст, увреждане по смисъла на Директива (ЕС) 2019/882 на Европейския парламент и на Съвета⁽¹⁶⁾ или конкретно социално или икономическо положение, което има вероятност да направи тези лица по-уязвими на експлоатация, като например лица, живеещи в крайна бедност, етнически или религиозни малцинства. Такива системи с ИИ могат да бъдат пуснати на пазара, пуснати в действие или използвани с цел или последици, изразяващи се в съществено изменение на поведението на дадено лице, и по начин, който причинява или има разумна вероятност да причини значителна вреда на това или на друго лице или групи лица, включително вреди, които могат да се натрупват с течение на времето, поради което следва да бъдат забранени. Може да не е възможно да се приеме, че

⁽¹⁶⁾ Директива (ЕС) 2019/882 на Европейския парламент и на Съвета от 17 април 2019 г. за изискванията за достъпност на продукти и услуги (ОВ L 151, 7.6.2019 г., стр. 70).

е налице намерение за изменение на поведението, когато изменението се дължи на фактори, външни за системата с ИИ, които са извън контрола на доставчика или внедрителя, а именно фактори, които може да не са разумно предвидими и поради това да не е възможно доставчикът или внедрителят на системата с ИИ да ги смекчи. Във всеки случай не е необходимо доставчикът или внедрителят да има намерение да причини значителна вреда, при условие че тази вреда произтича от манипулативни или експлоататорски практики, използващи ИИ. Забраните за такива практики в областта на ИИ допълват разпоредбите, съдържащи се в Директива 2005/29/ЕО на Европейския парламент и на Съвета⁽¹⁷⁾, по-специално за забрана при всички обстоятелства на неоялните търговски практики, водещи до икономически или финансови вреди за потребителите, независимо дали са въведени чрез системи с ИИ, или по друг начин. Забраните за манипулативни и експлоататорски практики в настоящия регламент не следва да засягат законните практики при медицинско лечение, като например психологическо лечение на психично заболяване или физическа рехабилитация, когато тези практики се извършват в съответствие с приложимото право и приложимите медицински стандарти, например за изричното съгласие на лицата или техните законни представители. Освен това общоприетите и законни търговски практики, например в областта на рекламата, които са в съответствие с приложимото право, не следва сами по себе си да се считат за вредни манипулативни практики, използващи ИИ.

- (30) Следва да бъдат забранени системите за биометрично категоризиране, които се основават на биометрични данни на физическите лица, като например лицето или пръстовите отпечатъци на дадено лице, за да се направят заключения или изводи относно неговите политически възгледи, членство в синдикални организации, религиозни или философски убеждения, раса, сексуален живот или сексуална ориентация. Тази забрана не следва да обхваща законното обозначаване, филтриране или категоризиране на наборите от биометрични данни, получени в съответствие с правото на Съюза или националното право въз основа на биометрични данни, като например сортиране на изображения според цвета на косата или цвета на очите, които могат да се използват например в правоохранителната област.
- (31) Системите с ИИ, осигуряващи социално оценяване на физически лица, извършено от публични или частни субекти, могат да доведат до дискриминационни резултати и изключване 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 физически лица или групи от такива лица въз основа на множество данни, свързани с тяхното социално поведение в различен контекст, или известни, изведени или предполагаеми лични или личностни характеристики, през определен период от време. Социалната класация, получена от такива системи с ИИ, може да доведе до увреждащо или неблагоприятно третиране на физически лица или на цели групи от такива лица в социален контекст, който няма връзка с контекста, в който първоначално са били генерирани или събрани данните, или до увреждащо третиране, което е непропорционално или неоправдано с оглед на тежестта, която се отдава на тяхното социално поведение. Поради това системите с ИИ, които включват такива неприемливи практики за оценяване и водещи до вредни или неблагоприятни резултати, следва да бъдат забранени. Тази забрана не следва да засяга законните практики за оценяване на физически лица, извършвани за конкретна цел в съответствие с правото на Съюза или националното право.
- (32) Използването на системи с ИИ за дистанционна биометрична идентификация в реално време на физически лица на обществено достъпни места за правоохранителни цели особено силно накърнява правата и свободите на засегнатите лица, доколкото то може да засегне личния живот на голяма част от населението, да породии усещане за постоянно наблюдение и косвено да действа разубеждаващо по отношение на упражняването на свободата на събранията и други основни права. Техническите неточности на системите с ИИ, предназначени за дистанционна биометрична идентификация на физически лица, могат да доведат до опорочени от предубеденост резултати и до дискриминация. Такива възможни опорочени от предубеденост резултати и дискриминационни последици са от особено значение по отношение на възраст, етническа принадлежност, раса, пол или увреждане. 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, които са засегнати при правоохранителните дейности или върху които тези дейности оказват въздействие.
- (33) Поради това използването на тези системи за правоохранителни цели следва да бъде забранено, освен в изчерпателно изброени и подробно определени ситуации, при които използването е строго необходимо за постигане на значителен обществен интерес, чиято важност надделява над рисковете. Тези ситуации включват издирването на някои жертви на престъпления, включително изчезнали лица; някои заплахи за живота или физическата безопасност на физически лица или от терористично нападение; както и установяването на местоположението или самоличността на извършители или заподозрени в извършването на престъпленията, изброени в приложение към настоящия регламент, когато тези престъпления се наказват в съответната държава членка с лишаване от свобода или мярка за задържане с

⁽¹⁷⁾ Директива 2005/29/ЕО на Европейския парламент и на Съвета от 11 май 2005 г. относно неоялни търговски практики от страна на търговци към потребители на вътрешния пазар и за изменение на Директива 84/450/ЕИО на Съвета, директиви 97/7/ЕО, 98/27/ЕО и 2002/65/ЕО на Европейския парламент и на Съвета и Регламент (ЕО) № 2006/2004 на Европейския парламент и на Съвета (Директива за неоялни търговски практики) (ОВ L 149, 11.6.2005 г., стр. 22).

максимален срок не по-малко от четири години, като се отчита определението на тези престъпления в правото 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 списъкът на престъпленията, поместен в приложение към настоящия регламент, се основава на 32-те престъпления, изброени в Рамково решение 2002/584/ПВР на Съвета⁽¹⁸⁾, като се отчита, че някои от тези престъпления на практика вероятно имат по-голямо значение от други, доколкото използването на дистанционна биометрична идентификация в реално време би могло да е вероятно необходимо и пропорционално в много различна степен с оглед на практическото установяване на местоположението или самоличността на извършителя или заподозрения за различните изброени престъпления, като се имат предвид също вероятните разлики в тяхната тежест, вероятност и размер на вредата или възможните отрицателни последици. Непосредствена заплаха за живота или физическата безопасност на физически лица може да възникне и от сериозно нарушаване на критична инфраструктура съгласно определението в член 2, точка 4 от Директива (ЕС) 2022/2557 на Европейския парламент и на Съвета⁽¹⁹⁾, когато нарушаването или унищожаването на такава критична инфраструктура би довело до непосредствена заплаха за живота или физическата безопасност на дадено лице, включително чрез сериозно увреждане на снабдяването с основни продукти за населението или на упражняването на основните функции на държавата. Освен това с настоящия регламент следва да се запази възможността правоохранителните органи, органите за граничен контрол, имиграционните органи или органите в областта на убежището да извършват проверки на самоличността в присъствието на засегнатото лице в съответствие с условията, определени в правото на Съюза и в националното право за такива проверки. По-специално, правоохранителните органи, органите за граничен контрол, имиграционните органи или органите в областта на убежището следва да могат да използват информационни системи, в съответствие с правото на Съюза или националното право, за установяване на самоличността на лица, които по време на проверка за установяване на самоличността отказват да бъде установена самоличността им или не са в състояние да посочат или докажат самоличността си, без настоящият регламент да изисква предварително разрешение с тази цел. Това може да бъде например лице, замесено в престъпление, което не желае или не може, поради злополука или здравословно състояние, да разкрие самоличността си пред правоохранителните органи.

- (34) 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 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 правоохранителни цели следва да бъде единствено с цел потвърждаване на самоличността на конкретно лице и следва да бъде ограничено до строго необходимото от гледна точка на срок, както и на териториален обхват и обхват по отношение на лицата, като се вземат предвид по-специално доказателствата или признаците за опасностите, жертвите или извършителя. Използването на системата за дистанционна биометрична идентификация в реално време на обществено достъпни места следва да бъде разрешено само ако съответният правоохранителен орган е извършил оценка на въздействието върху основните права и, освен ако в настоящия регламент не е предвидено друго, е регистрирал системата в базата данни, посочена в настоящия регламент. Референтната база данни на лицата следва да бъде подходяща за всеки случай на използване във всяка от посочените по-горе ситуации.

- (35) За всяко използване на система за дистанционна биометрична идентификация в реално време на обществено достъпни места за правоохранителни цели следва да се изисква изрично и конкретно разрешение от съдебен орган или от независим административен орган на държава членка, чието решение е задължително. Това разрешение следва по принцип да бъде получено преди използването на системата с ИИ с цел идентифициране на дадено лице или лица. Изключения от това правило следва да се допускат в надлежно обосновани спешни случаи, а именно в ситуации, при които необходимостта от използване на съответните системи е такава, че е практически и обективно невъзможно да бъде получено разрешение преди началото на използването на системата с ИИ. При такива спешни ситуации използването на системата с ИИ следва да бъде ограничено до абсолютно необходимия минимум и да е съпроводено с подходящи гаранции и условия, както са установени в националното право и специално указани в контекста на всеки отделен случай на спешно използване от самия правоохранителен орган. Освен това в такива ситуации правоохранителният орган следва да поиска такова разрешение, като посочи причините, поради които не е могъл да го поиска по-рано, без ненужно забавяне и най-късно в рамките на 24 часа. Ако искането за това разрешение бъде отхвърлено, използването на системи за биометрична идентификация в реално време, свързано с това разрешение, следва да бъде прекратено незабавно и всички данни, свързани с това използване, следва да бъдат премахнати и заличени. Тези данни включват входящите данни, получени пряко от система с ИИ в хода на използването на такава система, както и резултатите от използването, свързано с това разрешение. Това не следва да включва входящи данни,

⁽¹⁸⁾ 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).

⁽¹⁹⁾ Директива (ЕС) 2022/2557 на Европейския парламент и на Съвета от 14 декември 2022 г. за устойчивостта на критичните субекти и за отмяна на Директива 2008/114/ЕО на Съвета (ОВ L 333, 27.12.2022 г., стр. 164).

законно придобити в съответствие с друг правен акт на Съюза или национален правен акт. Във всеки случай решение, което поражда неблагоприятни правни последици за дадено лице, не следва да бъде взето единствено въз основа на резултата от системата за дистанционна биометрична идентификация.

- (36) За да изпълняват задачите си в съответствие с изискванията, установени в настоящия регламент, както и в националните правила, съответният орган за надзор на пазара и националният орган за защита на данните следва да бъдат уведомявани за всяко използване на системата за биометрична идентификация в реално време. Уведомените за това използване органи за надзор на пазара и национални органи за защита на данните следва да представят на Комисията годишен доклад относно използването на системи за биометрична идентификация в реално време.
- (37) 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 съответната държава членка е решила изрично да предвиди възможността за допускане на такова използване в подробните правила на националното си право. Следователно съгласно настоящия регламент държавите членки са свободни изобщо да не предвиждат такова възможност или да предвидят такова възможност само по отношение на някои от целите, посочени в настоящия регламент, които могат да оправдаят допустимото използване. Тези национални правила следва да бъдат съобщени на Комисията в срок от 30 дни след приемането им.
- (38) Използването на системи с ИИ за дистанционна биометрична идентификация в реално време на физически лица на обществено достъпни места за правоохранителни цели задължително включва обработването на биометрични данни. Правилата на настоящия регламент, които забраняват, с някои изключения, подобно използване и чието правно основание е член 16 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 урежда изчерпателно това използване и свързаното с него обработване на биометрични данни. Поради това такова използване и такова обработване следва да бъдат възможни само доколкото са съвместими с рамката, установена с настоящия регламент, без да има възможност извън тази рамка компетентните органи, когато действат с правоохранителни цели, да използват такива системи и да обработват такива данни във връзка с тях 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 (ЕС) 2016/680. Използването обаче на системи за дистанционна биометрична идентификация в реално време на обществено достъпни места за цели, различни от правоохранителни цели, включително от компетентни органи, не следва да бъде обхванато от специалната рамка относно такова използване за правоохранителни цели, установена с настоящия регламент. Поради това прямо използването за цели, различни от правоохранителни цели, не следва да се прилагат изискването за разрешение съгласно настоящия регламент и приложимите подробни правила на националното право, които може да уреждат това разрешение.
- (39) Всяко обработване на биометрични данни и други лични данни, необходимо за използването на системи с ИИ за биометрична идентификация, различно от обработване във връзка с използването на системи за дистанционна биометрична идентификация в реално време на обществено достъпни места за правоохранителни цели, уредено в настоящия регламент, следва да продължи да отговаря на всички изисквания, произтичащи от член 10 от Директива (ЕС) 2016/680. За цели, различни от правоохранителни цели, с член 9, параграф 1 от Регламент (ЕС) 2016/679 и член 10, параграф 1 от Регламент (ЕС) 2018/1725 се забранява обработването на биометрични данни, като се прилагат ограничени брой изключения, предвидени в посочените членове. В приложението на член 9, параграф 1 от Регламент (ЕС) 2016/679 използването на дистанционна биометрична идентификация за цели, различни от правоохранителни цели, вече е забранявано с решения на националните органи за защита на данните.
- (40) 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 правилата, предвидени в член 5, параграф 1, първа алинея, буква ж), доколкото се прилагат за използването на системи за биометрично категоризиране за дейности в областта на полицейското и съдебното сътрудничество по наказателноправни въпроси, в член 5, параграф 1, първа алинея, буква г), доколкото се прилагат за използването на системи с ИИ, обхванати от посочената разпоредба, в член 5, параграф 1, първа алинея, буква з) и параграфи 2 – 6 и в член 26, параграф 10 от настоящия регламент, приети на основание член 16 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 5 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 спазвани разпоредбите, установени на основание член 16 ДФЕС.
- (41) В съответствие с членове 2 и 2а от Протокол № 22 относно позицията на Дания, приложен към ДЕС и към ДФЕС, Дания не е обвързана и за нея не се прилагат правилата, предвидени в член 5, параграф 1, първа алинея, буква ж), доколкото се прилагат за използването на системи за биометрично категоризиране за дейности в областта на полицейското и съдебното сътрудничество по наказателноправни въпроси, в член 5, параграф 1, първа алинея, буква г), доколкото се прилагат за използването на системи с ИИ, обхванати от посочената разпоредба, в член 5,

параграф 1, първа алинея, буква з) и параграфи 2 – 6 и в член 26, параграф 10 от настоящия регламент, приети на основание член 16 от ДФЕС и 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 5 ДФЕС.

- (42) В съответствие с презумпцията за невиновност физическите лица в Съюза следва винаги да бъдат съдени въз основа на тяхното действително поведение. Физическите лица никога не следва да бъдат съдени въз основа на прогнозирано от ИИ поведение, базирано единствено на тяхното профилиране, личностни черти или характеристики, например гражданство, място на раждане, местопребиваване, брой деца, равнище на задлъжнялост или вид автомобил, без основателно подозрение за участието на лицето в престъпна дейност въз основа на обективни и проверими факти и без човешка оценка. Поради това следва да се забрани извършването на оценки на риска по отношение на физически лица, за да се оцени вероятността от извършване на престъпление или да се прогнозира извършването на действително или вероятно престъпление единствено въз основа на профилирането им или на оценката на техните личностни черти и характеристики. Във всеки случай тази забрана не се отнася до анализа на вероятността, който не се основава на профилирането на лица или на личностните черти и характеристики на тези лица, като например системи с ИИ, използващи анализ на риска за оценка на риска от финансови измами от страна на предприятия въз основа на подозрителни сделки или инструменти за анализ на риска за прогнозиране на вероятността за откриване на наркотици или незаконни стоки от страна на митническите органи, например въз основа на известни маршрути за трафик.
- (43) Пускането на пазара, пускането в действие за тази конкретна цел или използването на системи с ИИ, които създават или разширяват бази данни за разпознаване на лица чрез нецеленасочено извличане на лицеве изображения от интернет или записи от видеонаблюдение, следва да бъдат забранени, тъй като тази практика допринася за усещането за масово наблюдение и може да доведе до груби нарушения на основните права, включително правото на неприкосновеност на личния живот.
- (44) Съществуват сериозни опасения относно научната основа на системите с ИИ, които имат за цел да определят или да направят изводи за емоциите, по-специално като се има предвид, че изразяването на емоции се различава значително в отделните култури и ситуации и дори при едно и също лице. Сред основните недостатъци на тези системи са ограничената надеждност, липсата на съобразен с конкретния случай подход и ограничената възможност за обобщаване. Поради това системите с ИИ, които определят или правят изводи за емоциите или намеренията на физически лица въз основа на техните биометрични данни, могат да доведат до дискриминационни резултати и да накърнят правата и свободите на съответните лица. Като се има предвид властовото неравновесие в контекста на работата или образованието, съчетано с инвазивния характер на тези системи, подобни системи биха могли да доведат до увреждащо или неблагоприятно третиране на определени физически лица или на цели групи от такива лица. Поради това пускането на пазара, пускането в действие или използването на системи с ИИ, предназначени за определяне на емоционалното състояние на лица в ситуации, свързани с работното място и образованието, следва да бъдат забранени. Тази забрана не следва да обхваща системи с ИИ, пуснати на пазара единствено от медицински съображения или съображения, свързани с безопасността, като например системи, предназначени за терапевтична употреба.
- (45) Практиките, които са забранени от правото на Съюза, включително правото в областта на защитата на данните, недискриминацията и защитата на потребителите, както и правото в областта на конкуренцията, не следва да бъдат засегнати от настоящия регламент.
- (46) Високорисковите системи с ИИ следва да се пускат на пазара на Съюза, да се пускат в действие или да се използват 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 пораждат неприемливи рискове за важни обществени интереси на Съюза, признати и защитени от правото на Съюза. Въз основа на новата законодателна рамка, както е пояснено в известието на Комисията „Синьото ръководство“ за прилагане на правилата на ЕС относно продуктите – 2022 г. ⁽²⁰⁾, общото правило е, че повече от един правен акт от законодателството на Съюза за хармонизация, например регламенти (ЕС) 2017/745 ⁽²¹⁾ и (ЕС) 2017/746 ⁽²²⁾ на Европейския парламент и на Съвета или Директива 2006/42/ЕО на Европейския парламент и на Съвета ⁽²³⁾, може да е приложим за един продукт, тъй като предоставянето или пускането в действие може да се извърши само когато продуктът е в съответствие с цялото приложимо законодателство на Съюза за хармонизация. За

⁽²⁰⁾ ОВ С 247, 29.6.2022 г., стр. 1.

⁽²¹⁾ 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).

⁽²²⁾ 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).

⁽²³⁾ Директива 2006/42/ЕО на Европейския парламент и на Съвета от 17 май 2006 г. относно машините и за изменение на Директива 95/16/ЕО (ОВ L 157, 9.6.2006 г., стр. 24).

да се гарантира съгласуваност и да се избегне ненужна административна тежест или разходи, доставчиците на продукт, който съдържа една или повече високорискови системи с ИИ, за които се прилагат изискванията на настоящия регламент и на законодателството на Съюза за хармонизация, посочено в приложение към настоящия регламент, следва да разполагат с гъвкавост по отношение на оперативните решения за това как да се гарантира оптимално съответствие на продукт, който съдържа една или повече системи с ИИ, с всички приложими изисквания на законодателството на Съюза за хармонизация. Системите с ИИ, които се определят като високорискови, следва да се ограничат до имащите значително вредно въздействие върху здравето, безопасността и основните права на хората в Съюза, като при това следва да се свежда до минимум всяко възможно ограничаване на международната търговия.

- (47) Системите с ИИ биха могли да имат неблагоприятни последици за здравето и безопасността на хората, по-специално когато тези системи функционират като защитни елементи на продуктите. 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 се предлагат само безопасни и съответстващи на изискванията продукти – е важно да бъдат надлежно предотвратени и ограничени рисковете за безопасността, които могат да бъдат породени от даден продукт като цяло поради неговите цифрови компоненти, включително системи с ИИ. Например все по-автономните роботи, независимо дали в контекста на производството, или на личната помощ и грижи, следва да могат да работят и да изпълняват функциите си безопасно в сложна среда. По същия начин, в сектора на здравеопазването, където рисковете за живота и здравето са особено високи, все по-усъвършенстваните системи за диагностика и системите за подпомагане на човешките решения следва да бъдат надеждни и точни.
- (48) 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, правото на недискриминация, правото на образование, защитата на потребителите, правата на работниците, правата на хората с увреждания, равенството между половете, правата върху интелектуалната собственост, правото на ефективни правни средства за защита и на справедлив съдебен процес, правото на защита и презумпцията за невиновност, както и правото на добра администрация. В допълнение към тези права е важно да се подчертае факта, че децата имат специални права, които са залегнали в член 24 от Хартата и в Конвенцията на Организацията на обединените нации 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 благосъстояние. Основното право на високо равнище на опазване на околната среда, залегнало в Хартата и отразено в политиките на Съюза, също следва да се взема предвид при оценката на тежестта на вредата, която дадена система с ИИ може да причини, включително във връзка с човешкото здраве и безопасност.
- (49) По отношение на 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 Регламент (ЕО) № 300/2008 на Европейския парламент и на Съвета⁽²⁴⁾, Регламент (ЕС) № 167/2013 на Европейския парламент и на Съвета⁽²⁵⁾, Регламент (ЕС) № 168/2013 на Европейския парламент и на Съвета⁽²⁶⁾, Директива 2014/90/ЕС на Европейския парламент и на Съвета⁽²⁷⁾, Директива (ЕС) 2016/797 на Европейския парламент и на Съвета⁽²⁸⁾, Регламент (ЕС) 2018/858 на Европейския парламент и на Съвета⁽²⁹⁾, Регламент (ЕС) 2018/1139 на Европейския парламент и на Съвета⁽³⁰⁾
- ⁽²⁴⁾ 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).
- ⁽²⁵⁾ 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).
- ⁽²⁶⁾ Регламент (ЕС) № 168/2013 на Европейския парламент и на Съвета от 15 януари 2013 г. относно одобряването и надзора на пазара на дву-, три- и четириколесни превозни средства (ОВ L 60, 2.3.2013 г., стр. 52).
- ⁽²⁷⁾ Директива 2014/90/ЕС на Европейския парламент и на Съвета от 30 май 2014 г. относно морското оборудване и за отмяна на Директива 96/98/ЕО на Съвета (ОВ L 257, 28.8.2014 г., стр. 146).
- ⁽²⁸⁾ 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).
- ⁽²⁹⁾ 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).
- ⁽³⁰⁾ 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 (ЕО) № 3922/91 на Съвета (ОВ L 212, 22.8.2018 г., стр. 1).

и Регламент (ЕС) 2019/2144 на Европейския парламент и на Съвета⁽³¹⁾, е целесъобразно тези актове да бъдат изменени, за да се гарантира, че Комисията отчита – въз основа на техническата и регулаторна специфика на всеки сектор и без да има намеса в съществуващите механизми и органи за управление, оценяване на съответствието и контрол на прилагането, създадени съгласно горепосочените актове – задължителните изисквания за високорисковите системи с ИИ, установени в настоящия регламент, когато приема съответни делегирани актове или актове за изпълнение на основание на горепосочените актове.

- (50) По отношение на системите с ИИ, които са защитни елементи на продукти или които сами по себе си са продукти, попадащи в обхвата на определено законодателство на Съюза за хармонизация, посочено в приложение към настоящия регламент, е целесъобразно те да бъдат класифицирани като високорискови съгласно настоящия регламент, ако съответният продукт преминава през процедура за оценяване на съответствието с орган за оценяване на съответствието – трето лице, 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 отдых, въжени линии, уреди, захранвани с газово гориво, медицински изделия, медицински изделия за инвитро диагностика, автомобили и въздухоплавателни средства.
- (51) Класифицирането на дадена система с ИИ като високорискова съгласно настоящия регламент не следва непременно да означава, че продуктът, чийто защитен елемент 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 регламенти (ЕС) 2017/745 и (ЕС) 2017/746, в които се предвижда оценяване на съответствието от трето лице за продукти със среден и висок риск.
- (52) По отношение на самостоятелните системи с ИИ, а именно високорисковите системи с ИИ, различни от тези, които са защитни елементи на продукти или които сами по себе си са продукти, е целесъобразно 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 тежестта на възможната вреда, така и вероятността от настъпването ѝ, и тези системи с ИИ се използват в някои конкретно и предварително определени области, посочени в настоящия регламент. Идентифицирането на тези системи се основава на същата методика и критерии като предвидените и за евентуални бъдещи изменения на списъка на високорисковите системи с ИИ, които Комисията следва да бъде оправомощена да приеме чрез делегирани актове, за да се вземат предвид бързите темпове на технологично развитие, както и възможните промени в използването на системите с ИИ.
- (53) Важно е също така да се поясни, че може да има особени случаи, в които системите с ИИ, свързани с предварително определени области, посочени в настоящия регламент, не водят до значителен риск от увреждане на правните интереси, защитени в тези области, тъй като не оказват съществено влияние върху вземането на решения или не увреждат съществено тези интереси. За целите на настоящия регламент система с ИИ, която не оказва съществено влияние върху резултата от вземането на решения, следва да се разбира като система с ИИ, която не оказва въздействие върху същността, а оттам и върху резултата от вземането на решения, независимо дали е от човека, или автоматизирано. Системи с ИИ, която не оказва съществено влияние върху резултата от вземането на решения, може да включва ситуации, при които са изпълнени едно или повече от посочените по-нататък условия. Първото условие следва да бъде системата с ИИ да е предназначена да изпълнява конкретно определена процедурна задача, като например система с ИИ, която преобразува неструктурирани данни в структурирани данни, система с ИИ, която класифицира входящите документи в категории, или система с ИИ, която се използва за откриване на случаи на дублиране в рамките на голям брой приложения. Тези задачи са с толкова тесен и ограничен характер, че пораждаат само ограничени рискове, които не се увеличават чрез използването на система с ИИ в контекст, посочен като високорисково използване в приложение към настоящия регламент. Второто условие следва да бъде задачата,

⁽³¹⁾ Регламент (ЕС) 2019/2144 на Европейския парламент и на Съвета от 27 ноември 2019 г. относно изискванията за одобряване на типа на моторни превозни средства и техните ремаркета, както и на системи, компоненти и отделни технически възли, предназначени за такива превозни средства, по отношение на общата безопасност на моторните превозни средства 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 на регламенти (ЕО) № 631/2009, (ЕО) № 406/2010, (ЕО) № 672/2010, (ЕО) № 1003/2010, (ЕО) № 1005/2010, (ЕО) № 1008/2010, (ЕО) № 1009/2010, (ЕО) № 19/2011, (ЕО) № 109/2011, (ЕО) № 458/2011, (ЕО) № 65/2012, (ЕО) № 130/2012, (ЕО) № 347/2012, (ЕО) № 351/2012, (ЕО) № 1230/2012 и (ЕО) 2015/166 на Комисията (ОВ L 325, 16.12.2019 г., стр. 1).

изпълнявана от системата с ИИ, да има за цел подобряване на резултата от извършена преди това човешка дейност, която може да е от значение за целите на видовете високорисково използване, изброени в приложение към настоящия регламент. Като се имат предвид тези характеристики, системата с ИИ представлява само допълнение към човешката дейност с произтичащ от това понижен риск. Това условие например ще е приложимо при системи с ИИ, които имат за цел да подобрят езика, използван във вече изготвени документи, например във връзка с професионалния тон, академичния стил на езика или чрез привеждане на текста в съответствие с определено послание на дадена марка. Третото условие следва да бъде системата с ИИ да е предназначена да открива модели за вземане на решения или отклонения от съществуващи модели за вземане на решения. Рискът ще бъде намален, тъй като използването на системата с ИИ следва предварително извършена човешка оценка, която системата няма за цел да замени или да повлияе без подходящ преглед, извършен от човек. Тези системи с ИИ включват например такива, които, предвид определен модел на оценяване от преподавател, могат да се използват за последваща проверка на вероятността преподавателят да се е отклонил от модела на оценяване, така че да се открият възможни несъответствия или аномалии. Четвъртото условие следва да бъде системата с ИИ да е предназначена да изпълнява задача, която представлява само подготвителен етап преди извършването на оценка, която е от значение за целите на системите с ИИ, изброени в приложение в настоящия регламент, като по този начин възможното въздействие на резултата от системата намалява в значителна степен от гледна точка на това дали представлява риск за оценката, която ще последва. Това условие обхваща, наред с другото, интелигентни решения за обработка на файлове, които включват различни функции като индексирание, търсене, обработка на текст и реч или свързване на данни с други източници на данни, или системи с ИИ, използвани за превод на първоначални документи. Във всеки случай следва да се счита, че системи с ИИ, използвани в случаи на високорисково използване, посочени в приложение към настоящия регламент, пораждат значителни рискове от вреди за здравето, безопасността или основните права, ако системата с ИИ предполага профилиране по смисъла на член 4, точка 4 от Регламент (ЕС) 2016/679 или член 3, точка 4 от Директива (ЕС) 2016/680, или член 3, точка 5 от Регламент (ЕС) 2018/1725. За да се гарантират проследимост и прозрачност, доставчик, който счита, че дадена система с ИИ не е високорискова въз основа на посочените по-горе условия, следва да изготви документация за оценката, преди системата да бъде пусната на пазара или пусната в действие, и при поискване да предостави тази документация на националните компетентни органи. Този доставчик следва да бъде задължен да регистрира системата с ИИ в базата данни на ЕС, създадена съгласно настоящия регламент. С цел да се дадат допълнителни насоки за практическото изпълнение на условията, съгласно които системи с ИИ, изброени в приложение към настоящия регламент, по изключение не са високорискови, Комисията, след консултация със Съвета по ИИ, следва да предостави насоки, в които да се конкретизира това практическо изпълнение, допълнено от изчерпателен списък с практически примери за случаи на използване на системи с ИИ, които са високорискови, и такива, които не са.

- (54) Тъй като биометричните данни представляват специална категория лични данни, е целесъобразно да се класифицират като високорискови няколко случая на критично използване на биометрични системи, доколкото тяхното използване е разрешено съгласно съответното право на Съюза и национално право. Техническите неточности на системите с ИИ, предназначени за дистанционна биометрична идентификация на физически лица, могат да доведат до опорочени от предубеденост резултати и до дискриминация. Рискът от такива опорочени от предубеденост резултати и дискриминация е от особено значение във връзка с възраст, етническа принадлежност, раса, пол или увреждане. Поради това системите за дистанционна биометрична идентификация следва да бъдат класифицирани като високорискови с оглед на рисковете, които пораждат. Тази класификация изключва системите с ИИ, предназначени да бъдат използвани за биометрична проверка, включително за удостоверяване на самоличността, чиято единствена цел е да се потвърди, че конкретно физическо лице е лицето, за което се представя, и да се потвърди самоличността на физическо лице единствено за да се получи достъп до услуга, да се отключи устройство или да се придобие сигурен достъп до помещения. Освен това следва да бъдат класифицирани като високорискови системите с ИИ, предназначени да се използват за биометрично категоризиране в съответствие с чувствителни признаци или характеристики, защитени съгласно член 9, параграф 1 от Регламент (ЕС) 2016/679, въз основа на биометрични данни, доколкото те не са забранени съгласно настоящия регламент, и системи за разпознаване на емоции, които не са забранени съгласно настоящия регламент. Биометричните системи, които са предназначени да се използват единствено с цел да се позволи предприемането на мерки за киберсигурност и за защита на личните данни, не следва да се считат за високорискови системи с ИИ.
- (55) Във връзка с управлението и експлоатацията на критична инфраструктура, е целесъобразно системите с ИИ, предназначени да бъдат използвани като защитни елементи при управлението и експлоатацията на критична цифрова инфраструктура, посочена в точка 8 от приложението към Директива (ЕС) 2022/2557, 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. Защитните елементи на критичната инфраструктура, включително критичната цифрова инфраструктура, са системи, използвани за пряка защита на физическата цялост на критичната инфраструктура или на здравето и безопасността на хората и имуществото, но не са необходими за функционирането на системата. Аварията или

неизправността на тези елементи може пряко да породи рискове за физическата цялост на критичната инфраструктура и отгук –рискове за здравето и безопасността на хората и имуществото. Елементи, предназначени да се използват единствено за целите на киберсигурността, не следва да се квалифицират като защитни елементи. Сред примерите за защитни елементи на критичната инфраструктура могат да се посочат системите за наблюдение на водното налягане или контролните системи за пожароизвестяване в централите за изчисления в облак.

- (56) Внедряването на системи с ИИ в образованието е важно, за да се насърчи висококачествено цифрово образование и обучение и да се даде възможност на всички учещи се и преподаватели да придобиват и споделят необходимите цифрови умения и компетентности, включително за медийна грамотност и критично мислене, за да участват активно в икономиката, обществото и демократичните процеси. Същевременно системите с ИИ, използвани в образованието или професионалното обучение, по-специално за определяне на достъпа или приема, за разпределяне на места в институции или програми на всички нива на образованието и професионалното обучение, за оценяване на учебните резултати, за оценяване на подходящото ниво на образование за дадено лице и за оказване на съществено влияние върху нивото на образование и обучение, което лицата ще получат или до което ще могат да имат достъп, или за наблюдение и откриване на забранено поведение на ученици и студенти по време на изпити, следва да се класифицират като високорискови системи с ИИ, тъй като могат да определят образователния и професионалния път на дадено лице и така да повлияят на способността на това лице да осигурява прехраната си. Когато не са правилно проектирани и използвани, тези системи може да са особено инвазивни и е възможно да нарушат правото на образование и обучение, както и правото на недискриминация, и да продължат да възпроизвеждат исторически наложени дискриминационни модели, например срещу жени, определени възрастови групи, хора с увреждания или с определен расов или етнически произход или сексуална ориентация.
- (57) Системите с ИИ, използвани в областта на заетостта, управлението на работниците и достъпа до самостоятелна заетост, по-специално за подбор и наемане на лица, за вземане на решения, засягащи условията за повишение при отношения във връзка с полагане на труд и прекратяване на договорни отношения във връзка с полагане на труд, за разпределяне на задачи въз основа на индивидуално поведение, личностни черти или характеристики и за наблюдение 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, осигуряването на прехраната на тези лица и правата на работниците. Съответните договорни отношения във връзка с полагането на труд следва по пълноценен начин да включват и служителите и лицата, предоставящи услуги чрез платформи, както е посочено в работната програма на Комисията за 2021 г. По време на целия процес на набиране на персонал и при оценката, повишаването или задържането на лица в договорни отношения във връзка с полагането на труд такива системи могат да продължат да възпроизвеждат исторически наложени дискриминационни модели, например срещу жени, определени възрастови групи, хора с увреждания или с определен расов или етнически произход или сексуална ориентация. Системите с ИИ, използвани за наблюдение на работата и поведението на тези лица, могат също така да накърнят техните основни права на защита на данните и неприкосновеност на личния живот.
- (58) Друга област, в която използването на системи с ИИ заслужава специално внимание, е достъпът до и ползването на някои основни частни и публични услуги и подпомагане, необходими на хората за пълноценно участие в обществото или за подобряване на техния стандарт на живот. По-специално, физическите лица, които кандидатстват или получават основно обществено подпомагане и услуги от публични органи, а именно здравни услуги, социалноосигурителни обезщетения, социални услуги, осигуряващи закрила в случаи като майчинство, заболяване, трудова злополука, зависимост или старост и загуба на работа, както и на социална помощ и помощ за жилищно настаняване, обикновено зависят от това подпомагане и услуги и са в уязвимо положение по отношение на отговорните органи. Ако системите с ИИ се използват, за да се определи дали това подпомагане и услуги следва да бъдат предоставени, отказани, намалени, отменени или възстановени от органите, включително дали бенефициерите имат законно право да се ползват от това подпомагане или услуги, въпросните системи 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, и поради това следва да бъдат класифицирани като високорискови. Независимо от това настоящият регламент не следва да 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 пораждаат висок риск за юридическите и физическите лица. Наред с това 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. Използването за тези цели системи с ИИ могат да доведат до дискриминация на лица или групи и да продължат да възпроизвеждат исторически наложени дискриминационни модели, например въз основа на расов или етнически произход, пол, увреждане, възраст, сексуална ориентация, или да създадат нови форми на дискриминация. Системите с ИИ, предвидени в правото на Съюза за целите на разкриването на измами при предлагането на финансови услуги и за пруденциални цели за изчисляване на капиталовите изисквания на кредитните институции и застрахователите, не следва обаче да се считат за високорискови съгласно настоящия регламент. Освен това системите с ИИ, предназначени да се използват за оценка на риска и ценообразуване във връзка със здравно застраховане и животозастраховане на физически лица, също могат

да оказват значително въздействие върху осигуряването на прехраната на лицата и ако не са надлежно проектирани, разработени и използвани, могат да нарушат техните основни права и да доведат до сериозни последици за живота и здравето на хората, включително финансово изключване и дискриминация. И на последно място, системите с ИИ, използвани за оценка и класифициране на спешните повиквания от физически лица или за изпращане или определяне на приоритет по отношение на изпращането на службите за спешно реагиране, включително от полицията, пожарната и медицинската помощ, както и на системите за разпределяне на пациенти в областта на спешната здравна помощ, също следва да бъдат класифицирани като високорискови, тъй като те вземат решения в ситуации, които са изключително критични за живота и здравето на хората и за тяхното имущество.

- (59) Предвид техните функции и отговорност, действията на правоохранителните органи, включващи определени видове използване 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 своето функциониране, точност или надеждност или не е била правилно проектирана и изпитана преди да бъде пусната на пазара или по друг начин пусната в действие, тя може да избира лица по дискриминационен начин или по неправилен или необективен в друго отношение начин. Освен това упражняването на важни процесуални основни права, като правото на ефективни правни средства за защита и на справедлив съдебен процес, както и правото на защита и презумпцията за невинност, би могло да бъде възпрепятствано, по-специално когато системите с ИИ не са достатъчно прозрачни, разбираеми и документирани. Поради това е целесъобразно редица системи с ИИ, предназначени да бъдат използвани в правоохранителен контекст, 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, да се класифицират като високорискови, доколкото тяхното използване е разрешено съгласно съответното право на Съюза и национално право. С оглед на естеството на дейностите и свързаните с тях рискове тези високорискови системи с ИИ следва да включват по-специално системи с ИИ, предназначени да бъдат използвани от или от името на правоохранителните органи или от институции, органи, служби или агенции на Съюза в подкрепа на правоохранителните органи за оценка на риска дадено физическо лице да стане жертва на престъпления, например полиграфи и подобни инструменти, за оценка на надеждността на доказателствата в хода на разследването или наказателното преследване на престъпления, и, доколкото това не е забранено съгласно настоящия регламент, за оценка на риска дадено физическо лице да извърши нарушение или повторно нарушение не само въз основа на профилирането на физически лица или на оценката на личностни черти и характеристики или на минало престъпно поведение на физически лица или групи, както и за профилиране в хода на разкриването, разследването или наказателното преследване на престъпления. Системите с ИИ, специално предназначени да се използват за административни производства от данъчните и митническите органи, както и от звената за финансово разузнаване, изпълняващи административни задачи за анализ на информация съгласно правото на Съюза за борба с изпирането на пари, не следва да се класифицират като високорискови системи с ИИ, използвани от правоохранителните органи за целите на предотвратяването, разкриването, разследването и наказателното преследване на престъпления. Използването на инструменти с ИИ от страна на правоохранителните и други съответни органи не следва да се превръща във фактор, обуславящ неравенство или изключване. Въздействието на използването на инструменти с ИИ върху правата на защита на заподозрените лица не следва да се пренебрегва, по-специално трудностите при получаване на съдържателна информация относно функционирането на тези системи и произтичащите от това трудности при оспорване на резултатите от тях в съда, по-специално от страна на физически лица, срещу които се води разследване.

- (60) Системите с ИИ, използвани в управлението на миграцията, убежището и граничния контрол, засягат лица, 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, доколкото използването им е разрешено съгласно съответното право на Съюза и национално право, да бъдат класифицирани като високорискови системите с ИИ, предназначени да бъдат използвани от или от името на компетентните публични органи или от институции, органи, служби или агенции на Съюза, натоварени със задачи в областта на управлението на миграцията, убежището и граничния контрол, например полиграфи и подобни инструменти, за оценка на определени рискове, произтичащи от физически лица, които влизат на територията на държава членка или подават молба за виза или убежище, за подпомагане на компетентните публични органи при разглеждането, включително свързаната с това оценка на надеждността на доказателствата, 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, с цел откриване, разпознаване или установяване на самоличността на физически лица в контекста на управлението на миграцията, убежището и граничния контрол, с изключение на проверка на документите за пътуване. Системите с ИИ в областта на управлението на миграцията, убежището и граничния контрол, обхванати от настоящия регламент, следва да съответстват на съответните процедурни изисквания, установени в Регламент (ЕО) № 810/2009 на Европейския парламент и на Съвета⁽³²⁾, Директива 2013/32/ЕС на Европейския парламент и на Съвета⁽³³⁾ и друго

⁽³²⁾ 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).

⁽³³⁾ 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).

съответно право на Съюза. Системите с ИИ в контекста на управлението на миграцията, убежището и граничния контрол не следва при никакви обстоятелства да се използват от държавите членки или институциите, органите, службите или агенциите на Съюза като средство за заобикаляне на техните международни задължения съгласно Конвенцията на Организацията на обединените нации за статута на бежанците, съставена в Женева на 28 юли 1951 г. и изменена с Протокола от 31 януари 1967 г. Те не следва да се използват и за нарушаване по какъвто и да било начин на принципа на забрана за връщане или за отказ във връзка с безопасни и ефективни законни възможности за достъп до територията на Съюза, включително правото на международна закрила.

- (61) 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, за да се преодолеят рисковете от възможна предубеденост, грешки и непрозрачност, е целесъобразно да се класифицират като високорискови системите с ИИ, предназначени да бъдат използвани от орган на съдебна власт или от негово име, за да подпомагат органите на съдебна власт при проучването и тълкуването на фактите и правото и при прилагането на правото към конкретен набор от факти. Системите с ИИ, предназначени да бъдат използвани от органите за алтернативно разрешаване на спорове за тези цели, също следва да се считат за високорискови, когато резултатите от производството по алтернативно разрешаване на спорове пораждат правни последици за страните. Използването на инструменти с ИИ може да подпомогне, но не следва да заменя правомощията на съда за вземане на решения или независимостта на съдебната власт; окончателното вземане на решение трябва да продължи да бъде ръководено от човека. Класификацията на системите с ИИ като високорискови не следва обаче да обхваща системите с ИИ, предназначени за чисто спомагателни административни дейности, които не засягат самото правораздаване по отделните дела, като например анонимизиране или псевдонимизиране на съдебни решения, документи или данни, комуникация между персонала и административни задачи.
- (62) Без да се засягат правилата, предвидени в Регламент (ЕС) 2024/900 на Европейския парламент и на Съвета ⁽³⁴⁾, и с цел да се преодолеят рисковете от неправомерна външна намеса в упражняването на правото на глас, залегнало в член 39 от Хартата, и от неблагоприятните последици за демокрацията и принципите на правовата държава, системите с ИИ, предназначени да се използват за оказване на влияние върху резултата от избори или референдум или върху поведението на физическите лица при упражняване на правото им на глас в избори или референдум, следва да се класифицират като високорискови системи с ИИ, с изключение на системите с ИИ, на чиито резултати физическите лица не са пряко изложени, като например инструменти, използвани за организиране, оптимизиране и структуриране на политически кампании от административна и логистична гледна точка.
- (63) Фактът, че дадена система с ИИ е класифицирана като високорискова система с ИИ съгласно настоящия регламент, не следва да се тълкува като указване, че използването на системата е законосъобразно съгласно други актове на правото на Съюза или съгласно националното право, съвместимо с правото на Съюза, като например относно защитата на личните данни и 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 тълкува като предоставящ правно основание за обработването на лични данни, включително, ако е приложимо, на специални категории лични данни, освен когато в него изрично е предвидено друго.
- (64) За да се ограничат рисковете, произтичащи от високорискови системи с ИИ, пуснати на пазара или пуснати в действие, и за да се гарантира високо равнище на надеждност, за високорисковите системи с ИИ следва да се прилагат някои задължителни изисквания, при които се вземат предвид предназначението и контекстът на използване на системата с ИИ и които са съобразени със системата за управление на риска, която ще бъде създадена от доставчика. Мерките, предприети от доставчиците за спазване на задължителните изисквания на настоящия регламент, следва да са съобразени с общопризнатите съвременни технически постижения в областта на ИИ и да бъдат пропорционални и ефективни за постигане на целите на настоящия регламент. Въз основа на новата законодателна рамка, съгласно обясненията в известието на Комисията „Синьото ръководство“ за прилагане на правилата на ЕС относно продуктите – 2022 г., общото правило е, че повече от един правен акт от законодателството на Съюза за хармонизация може да е приложим за един продукт, тъй като предоставянето на пазара или пускането в действие може да се извърши само когато продуктът е в съответствие с цялото приложимо законодателство на Съюза за хармонизация. Опасностите, свързани със системите с ИИ, обхванати от изискванията на настоящия регламент, се отнасят до аспекти, различни от действащото законодателство на Съюза за хармонизация, поради което изискванията на настоящия регламент ще допълнят действащото законодателство на Съюза за хармонизация. Например машините или медицинските изделия, включващи система с ИИ, могат да представляват рискове, които не са обхванати от

⁽³⁴⁾ Регламент (ЕС) 2024/900 на Европейския парламент и на Съвета от 13 март 2024 г. относно прозрачността и таргетирането на политическото рекламиране (ОВ L, 2024/900, 20.3.2024 г., ELI: <https://eur-lex.europa.eu/eli/reg/2024/900/oj>).

съществени изисквания, свързани със здравето и безопасността, установени в съответното законодателство на Съюза за хармонизация, тъй като в това секторно право не се уреждат рисковете, присъщи за системите с ИИ. Поради това е необходимо едновременно и допълващо се прилагане на различните законодателни актове. За да се гарантира съгласуваност и да се избегнат ненужна административна тежест и ненужни разходи, доставчиците на продукт, който съдържа една или повече високорискови системи с ИИ, за които се прилагат изискванията на настоящия регламент и на законодателството на Съюза за хармонизация въз основа на новата законодателна рамка, което е посочено в приложение към настоящия регламент, следва да разполагат с гъвкавост по отношение на оперативните решения за това как да се гарантира оптимално съответствие на продукт, който съдържа една или повече системи с ИИ, с всички приложими изисквания на това законодателство на Съюза за хармонизация. Тази гъвкавост би могла да означава например решение на доставчика да интегрира част от необходимите процеси на изпитване и докладване, информация и документация, изисквани съгласно настоящия регламент, във вече съществуваща документация и процедури, изисквани съгласно съществуващото законодателство на Съюза за хармонизация въз основа на новата законодателна рамка, посочено в приложение към настоящия регламент. Това по никакъв начин не следва да засяга задължението на доставчика да спазва всички приложими изисквания.

- (65) Системата за управление на риска следва да се състои от непрекъснат цикличен процес, който се планира и протича през целия жизнен цикъл на високорисковата система с ИИ. Този процес следва да бъде насочен към установяване и ограничаване на съответните рискове, произтичащи от системите с ИИ, за здравето, безопасността и основните права. Системата за управление на риска следва да подлежи на редовен преглед и за бъде актуализирана, за да се гарантира непрекъснатата ѝ ефективност, както и обосновката и документирането на всички важни решения и действия, предприети съгласно настоящия регламент. Този процес следва да гарантира, че доставчикът установява рисковете или неблагоприятните въздействия и прилага мерки за ограничаване на известните и разумно предвидими рискове, произтичащи от системите с ИИ, за здравето, безопасността и основните права с оглед на тяхното предназначение и разумно предвидима неправилна експлоатация, включително възможните рискове, произтичащи от взаимодействието между системата с ИИ и средата, в която тя работи. Системата за управление на риска следва да предприема най-подходящите мерки за управление на риска с оглед на съвременните технически постижения в областта на ИИ. При определянето на най-подходящите мерки за управление на риска доставчикът следва да документира и обясни направения избор и, когато е целесъобразно, да включи експерти и външни заинтересовани страни. При установяването на разумно предвидима неправилна експлоатация на високорискови системи с ИИ доставчикът следва да обхване използването на системите с ИИ, които, макар и да не са пряко обхванати от предназначението и предвидени в инструкциите за употреба, може все пак да се очаква, че са резултат от лесно предвидимо човешко поведение в контекста на специфичните характеристики и използване на конкретна система с ИИ. Всички 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 породят рискове за здравето и безопасността или за основните права, следва да бъдат включени в инструкциите за употреба, предоставени от доставчика. Целта е да се гарантира, че внедрителят е запознат с тях и ги взема предвид при използването на високорисковата система с ИИ. Определянето и прилагането на мерки за ограничаване на риска в случаи на предвидима неправилна експлоатация съгласно настоящия регламент не следва да изискват осигуряването на конкретно допълнително обучение за високорисковата система с ИИ от страна на доставчика с цел намиране на решение във връзка с предвидимата неправилна експлоатация. Доставчиците обаче се насърчават да обмислят такива допълнителни мерки за обучение с цел ограничаване на случаи на разумно предвидима неправилна експлоатация, когато това е необходимо и целесъобразно.
- (66) По отношение на високорисковите системи с ИИ следва да се прилагат изисквания за управлението на риска, качеството и целесъобразността на използваните набори от данни, техническата документация и поддържането на регистри, прозрачността и предоставянето на информация на внедрителите, човешкият контрол, надеждността, точността и киберсикурността. Тези изисквания са необходими за ефективно ограничаване на рисковете за здравето, безопасността и основните права. Тъй като не съществуват други разумни, по-малко ограничителни мерки за търговията, тези изисквания не представляват необосновани ограничения на търговията.
- (67) Висококачествените данни и достъпът до тях имат жизненоважна роля за осигуряването на структура и за гарантирането на 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 обучителни, валидационни и изпитвателни данни изискват прилагането на подходящи практики за администриране и управление на данни. Наборите от обучителни, валидационни и изпитвателни данни, включително обозначенията, следва да бъдат подходящи, достатъчно представителни и във възможно най-голяма степен пълни и без грешки с оглед на предназначението на системата. За да се улесни спазването на правото на Съюза в областта на защитата на данните, като например Регламент (ЕС) 2016/679, практиките за администриране и управление на данни следва да включват, в случай на лични данни, прозрачност по отношение на първоначалната цел на събирането на данните. Наборите от данни следва също така да имат подходящи статистически свойства, включително по отношение на лицата или групите лица, във връзка с които е предназначена да се използва високорисковата система с ИИ, като се обръща специално внимание на намаляването на възможна предубеденост в наборите от данни, която има вероятност да засегне здравето и безопасността на хората, да окаже отрицателно въздействие върху основните права или да доведе до дискриминация, забранена съгласно правото на Съюза, особено когато резултатите от данните оказват влияние върху

входящите данни за бъдещи операции (обратни връзки). Предубедеността може например да бъде присъща за основните набори от данни, особено при използването или генерирането на исторически данни, когато системите се внедряват в реални условия. Резултатите, предоставени от системи с ИИ, могат да се повлияват от такава присъща предубеденост, при която съществува тенденция постепенно да се увеличава и по този начин да затвърждава и засилва съществуващата дискриминация, по-специално по отношение на лица, принадлежащи към определени уязвими групи, включително расови или етнически групи. Изискването наборите от данни да бъдат във възможно най-голяма степен пълни и без грешки не следва да засяга използването на техники за опазване на неприкосновеността на личния живот в контекста на разработването и изпитването на системи с ИИ. По-специално, наборите от данни следва да са съобразени, доколкото това се изисква с оглед на предназначението им, с особеностите, характеристиките или елементите, характерни за конкретната географска, контекстуална, поведенческа или функционална среда, в която системата с ИИ е предназначена да бъде използвана. Изискванията, свързани с администрирането на данни, могат да бъдат спазени чрез използване на услугите на трети лица, които предлагат сертифицирани услуги за осигуряване на съответствие, включително проверка на администрирането на данните, целостта на наборите от данни и практиките за обучение, валидиране и изпитване на данните, доколкото се гарантира спазването на изискванията за данните по настоящия регламент.

- (68) За разработването и оценката на високорискови системи с ИИ определени участници, като например доставчици, нотифицирани органи и други съответни субекти, например европейски цифрови иновационни центрове, структури за експериментирание и изпитване и научни работници, следва да имат достъп до и да използват висококачествени набори от данни в областите на дейност на тези участници, 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, валидирането 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 ИИ въз основа на тези набори от данни по сигурен, навременен, прозрачен и надежден начин, при който се запазва 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, валидирането и изпитването на системите с ИИ.
- (69) Правото на неприкосновеност на личния живот и на защита на личните данни трябва да бъде гарантирано през целия жизнен цикъл на системата с ИИ. В това отношение принципите на свеждане на данните до минимум и на защита на данните при проектирането и по подразбиране, определени в правото на Съюза в областта на защитата на данните, са приложими при обработването на лични данни. Мерките, предприети от доставчиците за гарантиране на спазването на тези принципи, могат да включват не само анонимизиране и криптиране, но и използване на технологии, които позволяват въвеждането на алгоритми в данните и позволяват обучение на системи с ИИ без предаване между страните или копиране на самите необработени или структурирани данни, без да се засягат изискванията за администриране на данните, предвидени в настоящия регламент.
- (70) За да се защитят правата на други лица от дискриминацията, която може да произтича от предубеденост в системите с ИИ, доставчиците следва по изключение, доколкото това е строго необходимо за целите на осигуряването на откриване и коригиране на предубедеността във високорисковите системи с ИИ, при спазване на подходящи гаранции за основните права и свободи на физическите лица и след прилагането на всички приложими условия, установени в настоящия регламент, в допълнение към условията, установени в регламенти (ЕС) 2016/679 и (ЕС) 2018/1725 и в Директива (ЕС) 2016/680, да могат да обработват и специални категории лични данни като въпрос от важен обществен интерес по смисъла на член 9, параграф 2, буква ж) от Регламент (ЕС) 2016/679 и член 10, параграф 2, буква ж) от Регламент (ЕС) 2018/1725.
- (71) Наличието на разбираема информация за начина на разработване на високорисковите системи с ИИ и начина на функционирането им през целия срок на експлоатация е от съществено значение, за да се даде възможност за проследимост на тези системи, проверка на съответствието с изискванията съгласно настоящия регламент, както и мониторинг на тяхното функциониране и мониторинг след пускането на пазара. Това изисква поддържането на регистри и наличието на техническа документация, съдържаща информация, която е необходима за оценяване на съответствието на системата с ИИ с приложимите изисквания и за улесняване на мониторинга след пускането на пазара. Тази информация следва да включва общите характеристики, способностите и ограниченията на системата, използваните алгоритми, данни и процеси на обучение, изпитване и валидиране, както и документация за съответната система за управление на риска, и следва да се изготвя в ясна и разбираема форма. Техническата документация следва да се актуализира по подходящ начин през целия срок на експлоатация на системата с ИИ. Освен това високорисковите системи с ИИ следва технически да позволяват автоматично записване на събития посредством записи по време на срока на експлоатация на системата.

- (72) За да се отговори на опасенията, свързани с непрозрачността и сложността на някои системи с ИИ, и да се помогне на внедрителите да изпълняват задълженията си съгласно настоящия регламент, следва да се изисква прозрачност за високорисковите системи с ИИ преди пускането им на пазара или пускането им в действие. Високорисковите системи с ИИ следва да бъдат проектирани по начин, който позволява на внедрителите да разберат как функционира системата с ИИ, да оценят нейната функционалност и да разберат нейните силни страни и ограничения. Високорисковите системи с ИИ следва да се придружават от подходяща информация под формата на инструкции за употреба. Тази информация следва да включва характеристиките, способностите и ограниченията на действието на системата с ИИ. Те ще обхващат информация относно възможните известни и предвидими обстоятелства, свързани с използването на високорисковата система с ИИ, включително действията от страна на внедрителя, които могат да повлияят на поведението и работата на системата и в рамките на които системата с ИИ може да породи рискове за здравето, безопасността и основните права, относно промените, които са предварително определени и чието съответствие е оценено от доставчика, както и относно съответните мерки за човешки контрол, включително мерките за улесняване на тълкуването на резултатите от системата с ИИ от внедрителите. Прозрачността, включително придружаващите инструкции за употреба, следва да подпомага внедрителите при използването на системата, както и при вземането на информирани решения. Внедрителите следва, наред с другото, да разполагат с по-добра възможност да направят правилния избор за системата, която възнамеряват да използват с оглед на приложимите за тях задължения, да бъдат запознати с предвиденото и неразрешеното използване и да използват системата с ИИ правилно и целесъобразно. За да се подобри разбираемостта и достъпността на информацията, включена в инструкциите за употреба, когато е целесъобразно следва да бъдат включени илюстративни примери, например относно ограниченията и относно предвиденото и неразрешеното използване на системата с ИИ. Доставчиците следва да гарантират, че цялата документация, включително инструкциите за употреба, съдържа съдържателна, изчерпателна, достъпна и разбираема информация, като се вземат предвид нуждите и предвидимите познания на внедрителите, за които е предназначена. Инструкциите за употреба следва да се предоставят на език, лесно разбираем за внедрителите, за които са предназначени, който е определен от съответната държава членка.
- (73) Високорисковите системи с ИИ следва да бъдат проектирани и разработени по такъв начин, че физическите лица да могат да следят тяхното функциониране, да гарантират, че те се използват по предназначение и че въздействието им се взема предвид през целия жизнен цикъл на системата. За тази цел доставчикът на системата следва да определи подходящи мерки за човешки контрол преди пускането ѝ на пазара или пускането ѝ в действие. По-специално, когато е целесъобразно, тези мерки следва да гарантират, че за системата се прилагат 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 контрол, разполагат с необходимата компетентност, обучение и авторитет за изпълнение на тази роля. Освен това е от съществено значение, когато е целесъобразно, да се гарантира, че високорисковите системи с ИИ включват механизми за даване на насоки и информация на дадено физическо лице, на което е възложен човешки контрол, за да взема информирани решения дали, кога и как да се намеси, за да се избегнат отрицателни последици или рискове, или да се спре системата, ако тя не функционира по предназначение. Предвид сериозните последици за хората в случай на неточно съвпадение, генерирано от някои системи за биометрична идентификация, е целесъобразно да се предвиди изискване за засилен човешки контрол над тези системи, така че внедрителят да не може да предприеме действие или да вземе решение въз основа на установена от системата самоличност, без това да е било проверено и потвърдено най-малко от две физически лица поотделно. Тези лица могат да се числят към един или повече образувания и да включват лицето, което управлява или използва системата. Това изискване не следва да поражда ненужна тежест или да води до забавяне; автоматичното вписване на отделните проверки, извършени от различните лица, в генерираните от системата записи би могло да е достатъчно. Като се имат предвид особеностите на правоохранителната област и областите на миграцията, граничния контрол и убежището, това изискване не следва да се прилага, когато според правото на Съюза или националното право се счита, че прилагането на това изискване е непропорционално.
- (74) Високорисковите системи с ИИ следва да функционират стабилно през целия си жизнен цикъл и да съответстват на подходящо ниво на точност, надеждност и киберсигурност, с оглед на тяхното предназначение и в съответствие с общопризнатите съвременни технически постижения. Комисията и съответните организации и заинтересовани страни се насърчават да вземат надлежно предвид ограничаването на рисковете и отрицателното въздействие на системата с ИИ. Очакваното ниво на показателите за ефективност следва да бъде обявено в придружаващите инструкции за употреба. Доставчиците се приканват да съобщават тази информация на внедрителите по ясен и лесно разбираем начин, без възможности за недоразумения или подвеждащи твърдения. Правото на Съюза в областта на законовата метрология, включително директиви 2014/31/ЕС⁽³⁵⁾ и 2014/32/ЕС⁽³⁶⁾ на Европейския парламент и на Съвета, има за цел да гарантира точността на измерванията и да спомогне за прозрачността и почтеността на търговските сделки. В този контекст, в сътрудничество със съответните заинтересовани страни и организации, като например органите по метрология и сравнителен анализ, Комисията следва да насърчава, когато е целесъобразно, разработването на сравнителни показатели и методики за измерване за системите с ИИ. При това Комисията следва да вземе под внимание и да си сътрудничи с международните партньори, работещи в областта на метрологията и съответните показатели за измерване, свързани с ИИ.

⁽³⁵⁾ Директива 2014/31/ЕС на Европейския парламент и на Съвета от 26 февруари 2014 г. за хармонизиране на законодателствата на държавите членки за предоставянето на пазара на везни с неавтоматично действие (ОВ L 96, 29.3.2014 г., стр. 107).

⁽³⁶⁾ Директива 2014/32/ЕС на Европейския парламент и на Съвета от 26 февруари 2014 г. за хармонизиране на законодателствата на държавите членки за предоставяне на пазара на средства за измерване (ОВ L 96, 29.3.2014 г., стр. 149).

- (75) Техническата надеждност е ключово изискване за високорисковите системи с ИИ. Те следва да бъдат устойчиви на вредно или друго нежелателно поведение, което може да се прояви в резултат на ограничения в системите или средата, в която те работят (например грешки, дефекти, несъответствия, неочаквани ситуации). Поради това следва да се предприемат технически и организационни мерки, за да се гарантира надеждността на високорисковите системи с ИИ, например чрез проектиране и разработване на подходящи технически решения за предотвратяване или свеждане до минимум на вредното или друго нежелателно поведение. Тези технически решения могат да включват например механизми, позволяващи на системата безопасно да прекъсне работата си (аварийни планове) при наличието на определени аномалии или когато работата се извършва извън предварително определени граници. 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 опорочени от предубеденост резултати, генерирани от системата с ИИ.
- (76) Киберсигурността има решаващо значение, за да се гарантира, че системите с ИИ са устойчиви на опити за промяна на тяхното използване, поведение или ефективност или за засягане на техните свойства, свързани със сигурността, от недобросъвестни трети лица, 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 (например чрез „отравяне на данните“) или обучени модели (например чрез враждебни атаки или изводи за принадлежност), или да използват уязвимите 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 високорискови системи с ИИ следва да предприемат подходящи мерки, например проверки на сигурността, като отчетат надлежно и основната ИКТ инфраструктура.
- (77) Без да се засягат изискванията, свързани с надеждността и точността, установени в настоящия регламент, при високорисковите системи с ИИ, които попадат в обхвата на регламент на Европейския парламент и на Съвета относно хоризонтални изисквания за киберсигурност за продукти с цифрови елементи, в съответствие с посочения регламент, може да се докаже съответствие с изискванията за киберсигурност на настоящия регламент, като се изпълнят същественият изисквания за киберсигурност, установени в посочения регламент. Когато високорисковите системи с ИИ съответстват на същественият изисквания на регламент на Европейския парламент и на Съвета относно хоризонтални изисквания за киберсигурност за продукти с цифрови елементи, те следва да се считат за съответстващи на изискванията за киберсигурност, установени в настоящия регламент, доколкото изпълнението на тези изисквания е доказано в ЕС декларацията за съответствие или части от нея, изготвена съгласно посочения регламент. За тази цел при оценката на рисковете за киберсигурността, свързани с продукт с цифрови елементи, класифициран като високорискова система с ИИ съгласно настоящия регламент, извършена съгласно регламент на Европейския парламент и на Съвета относно хоризонтални изисквания за киберсигурност за продукти с цифрови елементи, следва да се вземат предвид рисковете за киберустойчивостта на дадена система с ИИ по отношение на опитите на неоправомощени трети лица да променят нейното използване, поведение или работа, включително специфичните за ИИ уязвими места, като например „отравяне на данни“ или враждебни атаки, както и, ако е целесъобразно, рисковете за основните права, както се изисква в настоящия регламент.
- (78) Процедурата за оценяване на съответствието, предвидена в настоящия регламент, следва да се прилага по отношение на същественият изисквания за киберсигурност на даден продукт с цифрови елементи, попадащ в обхвата на регламент на Европейския парламент и на Съвета относно хоризонтални изисквания за киберсигурност за продукти с цифрови елементи и класифициран като високорискова система с ИИ съгласно настоящия регламент. Това правило обаче не следва да води до намаляване на необходимото ниво на увереност за критичните продукти с цифрови елементи, обхванати от регламент на Европейския парламент и на Съвета относно хоризонтални изисквания за киберсигурност за продукти с цифрови елементи. Поради това, чрез дерогация от това правило, за високорисковите системи с ИИ, които попадат в обхвата на настоящия регламент и които също така са определени като важни и критични продукти с цифрови елементи съгласно регламент на Европейския парламент и на Съвета относно хоризонтални изисквания за киберсигурност за продукти с цифрови елементи, и за които се прилага процедурата за оценяване на съответствието въз основа на вътрешен контрол, посочена в приложение към настоящия регламент, се прилагат разпоредбите за оценяване на съответствието, съдържащи се в регламент на Европейския парламент и на Съвета относно хоризонтални изисквания за киберсигурност за продукти с цифрови елементи, доколкото това се отнася до същественият изисквания за киберсигурност, установени в посочения регламент. В този случай за всички останали аспекти, обхванати от настоящия регламент, следва да се прилагат съответните разпоредби относно оценяването на съответствието въз основа на вътрешен контрол, установени в приложение към настоящия регламент. Въз основа на знанията и експертния опит на Агенцията на Европейския съюз за киберсигурност (ENISA) относно политиката в областта на киберсигурността и задачите, възложени на ENISA съгласно Регламент (ЕС) 2019/881 на Европейския парламент и на Съвета⁽³⁷⁾, Комисията следва да си сътрудничи с ENISA по въпроси, свързани с киберсигурността на системите с ИИ.

(37) 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. 15).

- (79) Целесъобразно е конкретно физическо или юридическо лице, определено като доставчик, да поеме отговорността за пускането на пазара или пускането в действие на дадена високорискова система с ИИ, независимо дали това физическо или юридическо лице е проектирало или разработило системата.
- (80) Като страни по Конвенцията на Организацията на обединените нации за правата на хората с увреждания Съюзът и държавите членки са правно задължени да защитават хората с увреждания от дискриминация и да насърчват тяхното равенство, да гарантират, че хората с увреждания имат достъп на равна основа с всички останали до информационни и комуникационни технологии и системи, и да гарантират зачитане на неприкосновеността на личния живот на хората с увреждания. Предвид нарастващото значение и използване на системи с ИИ прилагането на принципите за универсален дизайн за всички нови технологии и услуги следва да гарантира пълен и равен достъп на всички, които е възможно да бъдат засегнати от технологиите за ИИ или които ги използват, включително хората с увреждания, по начин, който изцяло отчита присъщото им достойнство и многообразие. Следователно е от съществено значение доставчиците да осигурят пълно съответствие с изискванията за достъпност, включително с Директива (ЕС) 2016/2102 на Европейския парламент и на Съвета⁽³⁸⁾ и Директива (ЕС) 2019/882. Доставчиците следва да осигурят съответствието с тези изисквания при проектирането. Поради това необходимите мерки следва да бъдат интегрирани във възможно най-голяма степен в проектирането на високорисковата система с ИИ.
- (81) 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. Доставчиците на високорискови системи с ИИ, които имат задължения по отношение на системите за управление на качеството съгласно съответното секторно право на Съюза, следва да имат възможност да включат елементите на системата за управление на качеството, предвидена в настоящия регламент, като част от съществуващата система за управление на качеството, предвидена в посоченото друго секторно право на Съюза. Взаимното допълване между настоящия регламент и действащото секторно право на Съюза също следва да бъде взето предвид в бъдещите дейности по стандартизация или в насоките, приемани от Комисията. Публичните органи, които пускат в действие 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, когато е целесъобразно, като вземат предвид особеностите на сектора и компетентността и организацията на съответния публичен орган.
- (82) 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 преди да се предоставят техните системи на пазара на Съюза, доставчиците, установени в трети държави, следва да определят с писмено пълномощно упълномощен представител, който е установен в Съюза. Този упълномощен представител има ключово значение за осигуряване на съответствието на високорисковите системи с ИИ, пуснати на пазара или пуснати в действие в Съюза от тези доставчици, които не са установени в Съюза, както и за изпълнение на функциите на лице за връзка, установено в Съюза.
- (83) С оглед на естеството и сложността на веригата за създаване на стойност за системите с ИИ и в съответствие с новата законодателна рамка, е от съществено значение да се гарантира правна сигурност и да се улесни спазването на настоящия регламент. Поради това е необходимо да се изяснят функциите и конкретните задължения на съответните оператори по веригата за създаване на стойност, като например вносителите и дистрибуторите, които могат да допринесат за разработването на системи с ИИ. В определени ситуации тези оператори биха могли да имат едновременно повече от една функция и поради това следва кумулативно да изпълняват всички съответни задължения, свързани с тези функции. Например даден оператор може да действа едновременно като дистрибутор и вносител.
- (84) За да се гарантира правна сигурност, е необходимо да се поясни, че при определени специфични условия всеки дистрибутор, вносител, внедрител или друго трето лице следва да се счита за доставчик на високорискова система с ИИ и следователно да поеме всички съответни задължения. Такъв би бил случаят, ако това лице постави името или търговската си марка върху високорискова система с ИИ, която вече е пусната на пазара или пусната в действие, без да се засягат споразумения, предвиждащи, че задълженията се разпределят по друг начин. Такъв би бил и случаят, ако това лице внесе съществено изменение във високорискова система с ИИ, която вече е пусната на пазара или пусната в действие, по такъв начин, че тя да продължи да бъде високорискова система с ИИ в съответствие с настоящия регламент, или ако измени предназначението на система с ИИ, включително система с ИИ с общо предназначение, която не е класифицирана като високорискова и вече е пусната на пазара или пусната в действие, по такъв начин, че системата с ИИ да стане високорискова система с ИИ в съответствие с настоящия регламент. Тези разпоредби следва да се прилагат, без да се засягат специалните разпоредби, установени в някои секторни законодателни актове на Съюза за хармонизация въз основа на новата законодателна рамка, заедно с които следва да се прилага настоящият регламент.

⁽³⁸⁾ Директива (ЕС) 2016/2102 на Европейския парламент и на Съвета от 26 октомври 2016 г. относно достъпността на уебсайтовете и мобилните приложения на организациите от обществен сектор (ОВ L 327, 2.12.2016 г., стр. 1).

Например член 16, параграф 2 от Регламент (ЕС) 745/2017, съгласно който определени изменения не следва да се считат за промени на изделие, които могат да се отразят на съответствието му с приложимите изисквания, следва да продължи да се прилага за високорисковите системи с ИИ, които са медицински изделия по смисъла на посочения регламент.

- (85) Системите с ИИ с общо предназначение могат да се използват като високорискови системи с ИИ сами по себе си или да бъдат компоненти на други високорискови системи с ИИ. Ето защо поради специфичното си естество и за да се гарантира справедливо разпределяне на отговорността по веригата за създаване на стойност в областта на ИИ, доставчиците на такива системи, независимо дали те могат да се използват сами по себе си като високорискови системи с ИИ от други доставчици, или като компоненти на високорискови системи с ИИ, и освен ако не е предвидено друго съгласно настоящия регламент, следва да си сътрудничат тясно с доставчиците на съответните високорискови системи с ИИ, за да им се даде възможност да спазват съответните задължения съгласно настоящия регламент, както и с компетентните органи, създадени съгласно настоящия регламент.
- (86) Когато съгласно условията, предвидени в настоящия регламент, доставчикът, който първоначално е пуснал на пазара системата с ИИ или я е пуснал в действие, вече не следва да се счита за доставчик за целите на настоящия регламент и когато този доставчик не е изключил изрично промяната на системата с ИИ във високорискова система с ИИ, първоначалният доставчик следва въпреки това да си сътрудничи тясно и да предостави необходимата информация, както и да осигури разумно очакваните технически достъп и друга помощ, които са необходими за изпълнението на задълженията, установени в настоящия регламент, по-специално по отношение на спазването на оценката на съответствието на високорисковите системи с ИИ.
- (87) Освен това когато високорискова система с ИИ, която е защитен елемент на продукт, попадащ в обхвата на законодателството на Съюза за хармонизация въз основа на новата законодателна рамка, не е пусната на пазара или пусната в действие независимо от продукта, производителят на продукта съгласно определението в съответното законодателство, следва да спазва задълженията на доставчика, установени в настоящия регламент, и следва по-специално да гарантира, че системата с ИИ, вградена в крайния продукт, съответства на изискванията на настоящия регламент.
- (88) В рамките на веригата за създаване на стойност в областта на ИИ множество лица често доставят системи, инструменти и услуги с ИИ, но също така и компоненти или процеси, които са интегрирани от доставчика в системата с ИИ с различни цели, включително обучение и повторно обучение на модели и изпитване и оценка на модели, интегриране в софтуера или други аспекти на разработването на модели. Тези лица заемат важно място във веригата за създаване на стойност по отношение на доставчика на високорисковата система с ИИ, в която са интегрирани техните системи, инструменти, услуги, компоненти или процеси с ИИ, и следва да предоставят чрез писмено споразумение на този доставчик необходимата информация, капацитет, технически достъп и друга помощ въз основа на общопризнатите съвременни технически постижения, за да се даде възможност на доставчика да изпълни изцяло задълженията, установени в настоящия регламент, без да се излагат на риск собствените им права върху интелектуалната собственост или търговски тайни.
- (89) Трети лица, които предоставят публичен достъп до инструменти, услуги, процеси или компоненти с ИИ, различни от модели на ИИ с общо предназначение, не следва да са задължени да спазват изискванията, насочени към отговорността по веригата за създаване на стойност в областта на ИИ, по-специално по отношение на доставчика, който ги е използвал или интегрирал, когато тези инструменти, услуги, процеси или компоненти с ИИ са достъпни в рамките на безплатен лиценз с отворен код. Разработчиците на безплатни инструменти, услуги, процеси или компоненти с ИИ с отворен код, различни от модели на ИИ с общо предназначение, следва да се насърчават да прилагат широко възприети практики за документиране, например карти за модели и информационни фишове, като начин за ускоряване на обмена на информация по веригата за създаване на стойност в областта на ИИ, което ще даде възможност да се популяризират надеждни системи с ИИ в Съюза.
- (90) Комисията би могла да разработи и препоръча незадължителни примерни договорни условия между доставчиците на високорискови системи с ИИ и трети лица, които доставят инструменти, услуги, компоненти или процеси, използвани или интегрирани във високорискови системи с ИИ, за да се улесни сътрудничеството по веригата за създаване на стойност. При разработването на незадължителни примерни договорни условия Комисията следва също така да взема предвид възможните договорни изисквания, приложими в конкретни сектори или стопански дейности.
- (91) 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 подходящ мониторинг на работата на дадена система с ИИ в реални условия, е целесъобразно да се определят конкретни отговорности за внедрителите. Внедрителите следва по-специално да предприемат подходящи технически и организационни мерки, за да гарантират, че използват високорискови системи с ИИ в съответствие с инструкциите за употреба, а също така следва да се предвидят някои други задължения по отношение на мониторинга на функционирането на системите с ИИ и по отношение на поддържането на регистри, когато е целесъобразно. Освен това внедрителите следва да гарантират, че лицата, на които е възложено да изпълняват инструкциите за употреба и човешкия контрол съгласно настоящия

регламент, притежават необходимата компетентност, по-специално подходящо ниво на грамотност, обучение и авторитет в областта на ИИ, за да изпълняват правилно тези задачи. Тези задължения не следва да засягат други задължения на внедрителите във връзка с високорискови системи с ИИ съгласно правото на Съюза или националното право.

- (92) Настоящият регламент не засяга задълженията на работодателите да информират или да информират и консултират работниците или техните представители съгласно правото и практиката на Съюза или националното право и практика, включително Директива 2002/14/ЕО на Европейския парламент и на Съвета ⁽³⁹⁾, относно решения за пускане в действие или използване на системи с ИИ. Продължава да е необходимо да се гарантира предоставянето на информация на работниците и техните представители относно планираното внедряване на високорискови системи с ИИ на работното място, когато не са изпълнени условията за тези задължения за информиране или информиране и консултиране, предвидени в други правни актове. Освен това подобно право на информиране допълва и е необходимо за постигането на целта за защита на основните права, залегнала в основата на настоящия регламент. Поради това в настоящия регламент следва да бъде предвидено изискване за информиране в този смисъл, без да се засягат съществуващите права на работниците.
- (93) Рисковете, свързани със системите с ИИ, могат да произтичат от начина, по който са проектирани тези системи, но могат да се дължат и на начина, по който се използват тези системи с ИИ. По тази причина внедрителите на високорискова система с ИИ имат решаващо значение за гарантиране на защитата на основните права, като допълват задълженията на доставчика при разработването на системата с ИИ. Внедрителите могат най-добре да разберат как конкретно ще бъде използвана високорисковата система с ИИ и следователно могат да установят потенциални значителни рискове, които не са били предвидени на етапа на разработване, тъй като разполагат с по-точни знания за контекста на използване и лицата или групите лица, които има вероятност да бъдат засегнати, включително уязвимите групи. Внедрителите на високорискови системи с ИИ, изброени в приложение към настоящия регламент, също имат решаващо значение за информирането на физическите лица и следва, когато вземат решения или подпомагат вземането на решения, свързани с физическите лица, когато е приложимо, да ги информират, че спрямо тях се използва високорискова система с ИИ. Тази информация следва да включва предназначението и вида на решенията, които се вземат. Внедрителят следва също така да информира физическите лица за правото им да получат обяснение, предвидено в настоящия регламент. По отношение на високорисковите системи с ИИ, използвани за правоохранителни цели, това задължение следва да се прилага в съответствие с член 13 от Директива (ЕС) 2016/680.
- (94) Всяко обработване на биометрични данни, свързано с използването на системи с ИИ за биометрична идентификация за правоохранителни цели, трябва да бъде в съответствие с член 10 от Директива (ЕС) 2016/680, който позволява такова обработване само когато това е строго необходимо, при спазване на подходящи гаранции за правата и свободите на субекта на данните, и когато това е разрешено от правото на Съюза или правото на държава членка. При такова разрешено използване трябва също така да се спазват принципите, установени в член 4, параграф 1 от Директива (ЕС) 2016/680, включително законосъобразност, добросъвестност и прозрачност, ограничаване в рамките на целта, точност и ограничаване на съхранението.
- (95) Без да се засяга приложимото право на Съюза, по-специално Регламент (ЕС) 2016/679 и Директива (ЕС) 2016/680, като се има предвид инвазивният характер на системите за последваща дистанционна биометрична идентификация, използването на тези системи следва да е придружено с гаранции. Системите за последваща дистанционна биометрична идентификация следва винаги да се използват по начин, който е пропорционален, законосъобразен и строго необходим, и следователно конкретизиран, по отношение на лицата, които трябва да бъдат идентифицирани, местоположението и времевия обхват, и въз основа на затворен набор от данни от законно придобити видеозаписи. Във всеки случай системите за последваща дистанционна биометрична идентификация не следва да се използват в правоохранителен контекст с цел неизбирателно наблюдение. Условията за последващата дистанционна биометрична идентификация не следва в никакъв случай да предоставят основание за заобикаляне на условията на забраната и строгите изключения по отношение на дистанционната биометрична идентификация в реално време.
- (96) За да се гарантира по ефективен начин защитата на основните права, внедрителите на високорискови системи с ИИ, които са публични органи, или частните субекти, предоставящи публични услуги, както и внедрителите на някои високорискови системи с ИИ, изброени в приложение към настоящия регламент, като например банкови институции или застрахователи, следва да извършват оценка на въздействието върху основните права преди пускането в действие. Услуги от обществен характер, които са от значение за физическите лица, могат да се предоставят и от частни субекти. Частните субекти, предоставящи такива публични услуги, са свързани с изпълнението на задачи от обществен интерес, например в областите на образованието, здравеопазването, социалните услуги, жилищното настаняване и правораждането. Целта на оценката на въздействието върху основните права е внедрителят да установи конкретните рискове за правата на лицата или групите лица, които е вероятно да бъдат засегнати, и да набележи мерките, които да бъдат предприети при настъпване на тези рискове. Оценката на въздействието следва да се извърши преди внедряването на

⁽³⁹⁾ Директива 2002/14/ЕО на Европейския парламент и на Съвета от 11 март 2002 г. за създаване на обща рамка за информиране и консултиране на работниците и служителите в Европейската общност (ОВ L 80, 23.3.2002 г., стр. 29).

високорисковата система с ИИ и следва да се актуализира, когато внедрителят счете, че някой от съответните фактори се е променил. В оценката на въздействието следва да се определят съответните процеси на внедрителя, в рамките на които високорисковата система с ИИ ще бъде използвана в съответствие с нейното предназначение, и следва да се посочи срокът, в който системата е предназначена да се използва, и честотата, с която тя е предназначена да се използва, както и конкретните категории физически лица и групи, които е вероятно да бъдат засегнати в конкретния контекст на използване. Оценката следва да включва и установяването на конкретните рискове от настъпване на вреди, които е вероятно да окажат въздействие върху основните права на тези лица или групи. При извършването на тази оценка внедрителят следва да вземе предвид информацията, която е от значение за правилната оценка на въздействието, включително, но не само, информацията, предоставена от доставчика на високорисковата система с ИИ в инструкциите за употреба. С оглед на установените рискове внедрителите следва да определят мерките, които да бъдат предприети при настъпване на тези рискове, включително например правила за управление в този конкретен контекст на използване, като например механизми за човешки контрол в съответствие с инструкциите за употреба или процедури за разглеждане на жалби и правна защита, тъй като те биха могли да бъдат от основно значение за ограничаване на рисковете за основните права в конкретни случаи на използване. След извършването на тази оценка на въздействието внедрителят следва да уведоми съответния орган за надзор на пазара. Когато е целесъобразно, за да се събере съответната информация, необходима за извършване на оценката на въздействието, внедрителите на високорисковата система с ИИ, по-специално когато системите с ИИ се използват в публичния сектор, биха могли да включат съответните заинтересовани страни, включително представители на групи лица, които е вероятно да бъдат засегнати от системата с ИИ, независими експерти и организации на гражданското общество, в извършването на такива оценки на въздействието и разработването на мерки, които да бъдат предприети в случай на настъпване на рисковете. Европейската служба по изкуствен интелект (наричана по-долу „Службата по ИИ“) следва да разработи образец на въпросник, за да се улесни спазването на изискванията и да се намали административната тежест за внедрителите.

- (97) Понятието „модел на ИИ с общо предназначение“ следва да бъде ясно определено и разграничено от понятието „системи с ИИ“, за да се гарантира правна сигурност. Определението следва да се основава на ключовите функционални характеристики на модел на ИИ с общо предназначение, по-специално общ характер и способност за компетентно изпълнение на широк набор от отделни задачи. Тези модели обикновено се обучават въз основа на голямо количество данни чрез различни методи, като например обучение (самообучение) със и без надзор и обучение с утвърждение. Моделите на ИИ с общо предназначение могат да бъдат пускани на пазара по различни начини, включително чрез библиотеки, приложно-програмни интерфейси (API), за директно изтегляне или с физическо копие. Тези модели могат да бъдат допълнително изменени или усъвършенствани в нови модели. Въпреки че моделите на ИИ са основни компоненти на системите с ИИ, сами по себе си те не представляват системи с ИИ. Моделите на ИИ изискват добавянето на допълнителни компоненти, като например потребителски интерфейс, за да се превърнат в системи с ИИ. Моделите на ИИ обикновено са интегрирани в системите с ИИ и са част от тях. В настоящия регламент се предвиждат специални правила за моделите на ИИ с общо предназначение и за моделите на ИИ с общо предназначение, пораждащи системни рискове, които следва да се прилагат и когато тези модели са интегрирани в система с ИИ или са част от нея. Приема се, че задълженията на доставчиците на модели на ИИ с общо предназначение следва да се прилагат след пускането на тези модели на пазара. Когато доставчикът на модел на ИИ с общо предназначение интегрира собствен модел в своя собствена система с ИИ, която се предоставя на пазара или се пуска в действие, този модел следва да се счита за пуснат на пазара и поради това задълженията, установени в настоящия регламент по отношение на моделите, следва да продължат да се прилагат в допълнение към задълженията за системите с ИИ. Задълженията, установени за моделите, във всички случаи не следва да се прилагат, когато собствен модел се използва за чисто вътрешни процеси, които не са от съществено значение за предоставянето на продукт или услуга на трети лица, и когато правата на физическите лица не са засегнати. Като се има предвид възможното им значително отрицателно въздействие, за моделите на ИИ с общо предназначение, пораждащи системен риск, следва винаги да се прилагат съответните задължения съгласно настоящия регламент. Определението не следва да обхваща модели на ИИ, използвани преди пускането им на пазара единствено с цел научноизследователска и развойна дейност и дейности по създаване на прототипи. Това не засяга задължението за спазване на настоящия регламент, когато след такива дейности на пазара се пуска модел.
- (98) Въпреки че общият характер на даден модел би могъл, наред с другото, да се определя и от редица параметри, следва да се счита, че модели с поне един милиард параметри, обучени с голямо количество данни и проявяващи в голяма степен самонадзор, се отличават със значителна степен на общ характер и компетентно изпълняват широк набор от отделни задачи.
- (99) Големите генеративни модели на ИИ са типичен пример за модел на ИИ с общо предназначение, като се има предвид, че те дават възможност за гъвкаво генериране на съдържание, например под формата на текст, аудиоматериали, изображения или видеоматериали, което лесно може да покрие широк спектър от отделни задачи.
- (100) Когато модел на ИИ с общо предназначение е интегриран в система с ИИ или е част от нея, тази система следва да се счита за система с ИИ с общо предназначение, когато поради тази интеграция системата е в състояние да обслужва най-различни цели. Системата с ИИ с общо предназначение може да бъде използвана пряко или може да бъде интегрирана в други системи с ИИ.

- (101) Доставчиците на модели на ИИ с общо предназначение имат особено значение и отговорност по веригата за създаване на стойност в областта на ИИ, тъй като моделите, които предоставят, могат да бъдат основа за набор от системи надолу по веригата, често предоставяни от доставчици надолу по веригата, които трябва добре да разбират моделите и техните способности, както за да могат да интегрират такива модели в своите продукти, така и за да изпълняват задълженията си съгласно настоящия или други регламенти. Поради това следва да се определят пропорционални мерки за прозрачност, включително изготвяне и актуализиране на документацията и предоставяне на информация относно модела на ИИ с общо предназначение за използването му от доставчиците надолу по веригата. Техническата документация следва да се изготвя и актуализира от доставчика на модели на ИИ с общо предназначение с цел предоставянето ѝ при поискване на Службата по ИИ и на националните компетентни органи. Минималният набор от елементи, които трябва да бъдат включени в тази документация, следва да бъде посочен в конкретни приложения към настоящия регламент. На Комисията следва да бъде предоставено правомощието да изменя тези приложения чрез делегирани актове с оглед на технологичното развитие.
- (102) Софтуер и данни, включително модели, предоставени с безплатен лиценз с отворен код, който им позволява да бъдат споделяни свободно и чрез който ползвателите могат свободно да ги достъпват, използват, променят и разпространяват в променен или непроменен вид, могат да допринесат за научните изследвания и иновациите на пазара и да осигурят значителни възможности за растеж на икономиката на Съюза. Следва да се обмисли използването на модели на ИИ с общо предназначение, представени с безплатни лицензи с отворен код, за да се гарантират високи равнища на прозрачност и отвореност, ако техните параметри, включително теглата, информацията за архитектурата на модела и информацията за използването на модела са публично достъпни. Лицензът следва да се счита за безплатен и с отворен код и когато дава възможност на ползвателите да използват, копират, разпространяват, изучават, променят и подобряват софтуер и данни, включително модели, при условие че се посочва първоначалният доставчик на модела и се спазват еднакви или сходни условия на разпространение.
- (103) Безплатните компоненти с ИИ с отворен код обхващат софтуера и данните, включително модели и модели, инструменти, услуги или процеси с ИИ с общо предназначение на дадена система с ИИ. Безплатните компоненти с ИИ с отворен код могат да бъдат предоставяни по различни начини, включително чрез разработването им в хранилища със свободен достъп. За целите на настоящия регламент компонентите с ИИ, които се предоставят срещу заплащане или се вземездяват по друг начин, включително чрез предоставянето на техническа поддръжка или други услуги, включително чрез софтуерна платформа, свързани с компонента с ИИ, или използването на лични данни по причини, различни от изключителната цел за подобряване на сигурността, съвместимостта или оперативната съвместимост на софтуера, с изключение на сделките между микропредприятията, не следва да се ползват от изключенията, предвидени за безплатните компоненти с ИИ с отворен код. Предоставянето на компоненти с ИИ чрез хранилища със свободен достъп не следва само по себе си да представлява вземездяване.
- (104) За доставчиците на модели на ИИ с общо предназначение, които са предоставени с безплатен лиценз с отворен код и чиито параметри, включително теглата, информацията за архитектурата на модела и информацията за използването на модела, са публично достъпни, следва да се прилагат изключения по отношение на свързаните с прозрачността изисквания, наложени на моделите на ИИ с общо предназначение, освен когато може да се счита, че те пораждаат системен риск, като в този случай обстоятелството, че моделът е прозрачен и придружен от лиценз с отворен код, не следва да се счита за достатъчна причина за изключване на спазването на задълженията съгласно настоящия регламент. Във всеки случай, като се има предвид, че предоставянето на модели на ИИ с общо предназначение с безплатен лиценз с отворен код не разкрива непременно съществена информация относно набора от данни, използван за обучението или финото регулиране на модела, и относно това как по този начин се гарантира спазването на авторското право, предвиденото за моделите на ИИ с общо предназначение изключение от съответствието с изискванията, свързани с прозрачността, не следва да се отнася до задължението за изготвяне на обобщение на съдържанието, използвано за обучение на модели, и задължението за въвеждане на политика за спазване на правото на Съюза в областта на авторското право, по-специално за установяване и съблюдаване на запазването на права съгласно член 4, параграф 3 от Директива (ЕС) 2019/790 на Европейския парламент и на Съвета⁽⁴⁰⁾.
- (105) Моделите на ИИ с общо предназначение, по-специално големите генеративни модели на ИИ, способни да генерират текст, изображения и друго съдържание, представляват уникални възможности за иновации, но също така са свързани и с трудности за хората на изкуството, авторите и другите творци, както и за начина, по който тяхното творческо съдържание се създава, разпространява, използва и потребява. Разработването и обучението на такива модели изисква достъп до големи количества текст, изображения, видеоматериали и други данни. Техниките за извличане на информация от текст и данни могат да се използват широко в този контекст за извличане и анализ на такова съдържание, което може да бъде защитено с авторско право и сродните му права. Всяко използване на защитено с авторско право съдържание изисква разрешение от съответните носители на права, освен ако не се прилагат съответните изключения и ограничения, свързани с авторското право. С Директива (ЕС) 2019/790 бяха въведени изключения и ограничения, които позволяват възпроизвеждането и извличането на откъси от произведения или

⁽⁴⁰⁾ Директива (ЕС) 2019/790 на Европейския парламент и на Съвета от 17 април 2019 г. относно авторското право и сродните му права в цифровия единен пазар и за изменение на директиви 96/9/ЕО и 2001/29/ЕО (ОВ L 130, 17.5.2019 г., стр. 92).

други обекти за целите на извличането на информация от текст и данни при определени условия. Съгласно тези правила носителите на права могат да изберат да запазят правата си върху своите произведения или други обекти, за да предотвратят извличането на информация от текст и данни, освен ако това не се извършва за целите на научни изследвания. Когато правото на отказ е изрично запазено по подходящ начин, доставчиците на модели на ИИ с общо предназначение трябва да получат разрешение от носителите на права, ако желаят да извършват извличане на информация от текст и данни за такива произведения.

- (106) Доставчиците, които пускат на пазара на Съюза модели на ИИ с общо предназначение, следва да гарантират спазването на съответните задължения, установени в настоящия регламент. За тази цел доставчиците на модели на ИИ с общо предназначение следва да въведат политика за спазване на правото на Съюза в областта на авторското право и сродните му права, по-специално за установяване и съблюдуване на запазването на права, изразено от носителите на права съгласно член 4, параграф 3 от Директива (ЕС) 2019/790. Всеки доставчик, който пуска на пазара на Съюза модел на ИИ с общо предназначение, следва да спазва това задължение, независимо от юрисдикцията, в която се извършват действията, свързани с авторското право, които са в основата на обучението на тези модели на ИИ с общо предназначение. Това е необходимо, за да се гарантира равнопоставеност на доставчиците на модели на ИИ с общо предназначение, при което нито един доставчик не следва да може да получи конкурентно предимство на пазара на Съюза чрез прилагане на по-ниски стандарти в областта на авторското право от предвидените в Съюза.
- (107) За да се повиши прозрачността по отношение на данните, които се използват при предварителното обучение и обучението на модели на ИИ с общо предназначение, включително текст и данни, защитени от правото в областта на авторското право, е целесъобразно доставчиците на такива модели да изготвят и оповестяват публично достатъчно подробно обобщение на съдържанието, използвано за обучение на модела на ИИ с общо предназначение. Като се отчита надлежно необходимостта от защита на търговските тайни и поверителната търговска информация, това обобщение следва като цяло да бъде изчерпателно по своя обхват, а не технически подробно, за да улесни лицата със законни интереси, включително носителите на авторски права, да упражняват и прилагат правата си съгласно правото на Съюза, например чрез изброяване на основните събрани данни или набори от данни, които са използвани при обучението по модела, като например големи частни или публични бази данни или архиви с данни, и чрез предоставяне на описателно разяснение за други използвани източници на данни. Целесъобразно е Службата по ИИ да осигури образец на обобщението, който следва да бъде опростен, ефективен и да позволява на доставчика да предостави изискваното обобщение в описателна форма.
- (108) По отношение на задълженията, наложени на доставчиците на модели на ИИ с общо предназначение, да въведат политика за спазване на правото на Съюза в областта на авторското право и да оповестят публично обобщение на съдържанието, използвано за обучението, Службата по ИИ следва да следи дали доставчикът е изпълнил тези задължения, без да проверява или да извършва оценка на обучителните данни за всяко отделно произведение от гледна точка на спазването на авторското право. Настоящият регламент не засяга прилагането на правилата в областта на авторското право, предвидени в правото на Съюза.
- (109) Спазването на задълженията, приложими за доставчиците на модели на ИИ с общо предназначение, следва да бъде съизмеримо и пропорционално на вида доставчик на модели, като се изключва необходимостта от спазването им за лицата, които разработват или използват модели за непрофесионални или научноизследователски цели, които въпреки това следва да бъдат насърчавани да спазват тези изисквания на доброволна основа. Без да се засяга правото на Съюза в областта на авторското право, спазването на тези задължения следва да е надлежно съобразено с размера на доставчика и да дава възможност за опростени начини за постигане на съответствие за МСП, включително новосъздадени предприятия, които не следва да представляват прекомерни разходи и да не възпират използването на такива модели. В случай на изменение или фино регулиране на даден модел задълженията на доставчиците на модели на ИИ с общо предназначение следва да бъдат ограничени до това изменение или фино регулиране, например чрез допълване на вече съществуващата техническа документация с информация за измененията, включително нови източници на обучителни данни, като начин да се гарантира спазването на задълженията по веригата за създаване на стойност, предвидени в настоящия регламент.
- (110) Моделите на ИИ с общо предназначение биха могли да породят системни рискове, които включват, но не се ограничават до действителни или разумно предвидими отрицателни последици във връзка с големи аварии, смущения в критични сектори и сериозни последици за общественото здраве и безопасност; действителни или разумно предвидими отрицателни последици за демократичните процеси, обществената и икономическата сигурност; разпространението на незаконно, невярно или дискриминационно съдържание. Следва да се приеме, че системните рискове нарастват заедно със способностите и обхвата на модела, могат да възникнат по време на целия жизнен цикъл на модела и се влияят от условията на неправилна експлоатация, надеждността, добросъвестността и сигурността на модела, степента на автономност на модела, неговия достъп до инструменти, новите или комбинирания условия,

стратегии за предоставяне и разпространение, възможността за премахване на предпазните механизми и други фактори. По-специално, досега международните подходи са установили необходимостта да се обърне внимание на рисковете, произтичащи от възможна умишлена неправилна експлоатация или непреднамерени проблеми с контрола, свързан с приважането в съответствие с човешките намерения; химичните, биологичните, радиологичните и ядрените рискове, като например начините, по които могат да бъдат намалени пречките за достъп, включително за разработване, придобиване на дизайн или използване на оръжия; офанзивните киберспособности, като например средствата, позволяващи откриване, експлоатация или оперативно използване на уязвими места; последиците от взаимодействието и използването на инструменти, включително например капацитета за контрол на физическите системи и за намеса в критичната инфраструктура; рисковете, свързани с възможността моделите да изготвят свои собствени копия, да се самовъзпроизвеждат или да обучават други модели; начините, по които моделите могат да доведат до вредна предубеденост и дискриминация с рискове за физически лица, общности или общества; улесняването на дезинформацията или накръняването на неприкосновеността на личния живот чрез заплахи за демократичните ценности и правата на човека; риска дадено събитие да доведе до верижна реакция със значителни отрицателни последици, които биха могли да засегнат цял град, цяла област на дейност или цяла общност.

- (111) Целесъобразно е да се създаде методика за класифициране на моделите на ИИ с общо предназначение като модели на ИИ с общо предназначение, пораждащи системен риск. Тъй като системните рискове произтичат от особено големи способности, следва да се счита, че моделът на ИИ с общо предназначение поражда системни рискове, ако има способности с висока степен на въздействие, оценени въз основа на подходящи технически инструменти и методики, или значително въздействие върху вътрешния пазар поради своя обхват. Способностите с висока степен на въздействие при моделите на ИИ с общо предназначение означава способности, които съответстват на или надхвърлят способностите, регистрирани в най-напредналите модели на ИИ с общо предназначение. Пълният набор от способности на даден модел би могъл да бъде по-добре разбран след пускането му на пазара или при взаимодействието на внедрителите с модела. В зависимост от съвременните технически постижения към момента на влизане в сила на настоящия регламент общото количество изчисления, използвани за обучението на модела на ИИ с общо предназначение, измерено при операции с плаваща запетая, е една от значимите приблизителни стойности за способностите на модела. Общото количество изчисления, използвано за обучение, включва изчисленията, използвани за всички дейности и методи, които са предназначени да подобрят способностите на модела преди внедряването, като например първоначално обучение, генериране на синтетични данни и фино регулиране. Поради това следва да се определи първоначален праг за операции с плаваща запетая, който, ако бъде достигнат от даден модел на ИИ с общо предназначение, води до презумпцията, че това е модел на ИИ с общо предназначение, пораждащ системен риск. Този праг следва да бъде коригиран с течение на времето, за да отразява технологичните и промишлените промени, като например подобрения в алгоритмите или повишена ефективност на хардуера, и следва да бъде допълван с референтни стойности и показатели за способностите на модела. За тази цел Службата по ИИ следва да работи с научната общност, стопанския сектор, гражданското общество и други експерти. Праговете, както и инструментите и референтните показатели за оценка на способностите с висока степен на въздействие следва да бъдат добри прогностични фактори за общия характер, способностите и свързания системен риск на моделите на ИИ с общо предназначение и биха могли да вземат предвид начина, по който моделът ще бъде пуснат на пазара, или броя на ползвателите, които той може да засегне. За да се допълни тази система, Комисията следва да има възможност да взема индивидуални решения за определяне на модел на ИИ с общо предназначение като модел на ИИ с общо предназначение, пораждащ системен риск, ако се установи, че този модел има способности или въздействие, равностойни на тези, обхванати от определения праг. Това решение следва да се вземе въз основа на цялостна оценка на критериите за определяне на модели на ИИ с общо предназначение, пораждащи системен риск, посочени в приложение към настоящия регламент, като например качество или размер на набора от обучителни данни, брой на бизнес ползвателите и крайните ползватели, свързаните с него условия за входящи данни и резултати, степен на автономност и възможности за увеличаване на мащаба или инструментите, до които той има достъп. При обосновано искане от доставчик, чийто модел е определен като модел на ИИ с общо предназначение, пораждащ системен риск, Комисията следва да вземе предвид искането и може да реши да направи нова преценка дали все още може да се счита, че моделът на ИИ с общо предназначение поражда системни рискове.
- (112) Необходимо е също така да се изясни процедурата за класифициране на модел на ИИ с общо предназначение, пораждащ системен риск. Модел на ИИ с общо предназначение, който отговаря на приложимия праг за способности с висока степен на въздействие, следва да се счита за модел на ИИ с общо предназначение, пораждащ системен риск. Доставчикът следва да уведоми Службата по ИИ най-късно две седмици след като бъдат изпълнени изискванията или стане известно, че даден модел на ИИ с общо предназначение ще отговаря на изискванията, свързани с презумпцията. Това е от особено значение във връзка с прага на операции с плаваща запетая, тъй като обучението на модели на ИИ с общо предназначение преминава през значително планиране, което включва предварително разпределяне на изчислителните ресурси, и следователно доставчиците на модели на ИИ с общо предназначение са в състояние да знаят дали техният модел би достигнал прага преди завършване на обучението. В контекста на това уведомяване доставчикът следва да може да докаже, че поради конкретните си характеристики даден модел на ИИ с общо предназначение по изключение не поражда системни рискове и че поради това не следва да бъде класифициран като модел на ИИ с общо предназначение, пораждащ системен риск. Тази информация е ценна, за да даде възможност на Службата по ИИ да предвиди пускането на пазара на модели на ИИ с общо предназначение, пораждащи системен

риск, а на доставчиците да могат да започнат работа със Службата по ИИ на ранен етап. Информацията е особено важна по отношение на модели на ИИ с общо предназначение, за които се планира да бъдат пуснати с отворен код, като се има предвид, че след пускането на модел с отворен код може да е по-трудно да се приложат необходимите мерки за гарантиране на спазването на задълженията съгласно настоящия регламент.

- (113) Ако на Комисията стане известен фактът, че даден модел на ИИ с общо предназначение отговаря на изискванията за класифициране като модел ИИ с общо предназначение, пораждащ системен риск, който преди това не е бил известен или за който съответният доставчик не е уведомил Комисията, на Комисията следва да бъде предоставено правомощието да го определи като такъв. Системата за приоритетни сигнали следва да гарантира, че Службата по ИИ е информирана от експертната група за модели на ИИ с общо предназначение, които евентуално следва да бъдат класифицирани като модели на ИИ с общо предназначение, пораждащи системен риск, в допълнение към дейностите по мониторинг на Службата по ИИ.
- (114) За доставчиците на модели на ИИ с общо предназначение, пораждащи системни рискове, следва да се прилагат, в допълнение към задълженията, предвидени за доставчиците на модели на ИИ с общо предназначение, задължения, насочени към установяване и ограничаване на тези рискове и осигуряване на подходящо равнище на защита на киберсигурността, независимо дали тези модели се предоставят като самостоятелни модели, или са вградени в система с ИИ или продукт. За постигането на тези цели настоящият регламент следва да изисква от доставчиците да извършват необходимите оценки на модела, по-специално преди първото му пускане на пазара, включително провеждане и документиране на конкурентно изпитване на модели, когато е целесъобразно и чрез вътрешни или независими външни изпитвания. Освен това доставчиците на модели на ИИ с общо предназначение, пораждащи системен риск, следва непрекъснато да оценяват и ограничават системните рискове, включително например чрез въвеждане на политики за управление на риска, като например процеси на отчетност и администриране, проследяване след пускането на пазара, предприемане на подходящи мерки през целия жизнен цикъл на модела и сътрудничество със съответните участници по веригата за създаване на стойност в областта на ИИ.
- (115) Доставчиците на модели на ИИ с общо предназначение, пораждащи системен риск, следва да оценяват и ограничават възможните системни рискове. Ако въпреки усилията за установяване и предотвратяване на рискове, свързани с модел на ИИ с общо предназначение, който може да поражда системни рискове, разработването или използването на модела причини сериозен инцидент, доставчикът на модел на ИИ с общо предназначение следва без ненужно забавяне да проследи инцидента и да докладва на Комисията и на националните компетентни органи за всяка съответна информация и възможни коригиращи действия. Освен това доставчиците следва да гарантират подходящо равнище на защита на киберсигурността на модела и неговата физическа инфраструктура, ако е целесъобразно, през целия жизнен цикъл на модела. Защитата на киберсигурността от системни рискове, свързани с недобросъвестно използване или атаки, следва надлежно да отчита случайни фактори като изтичане на модел, неразрешено предоставяне, заобикаляне на мерките за безопасност и защита срещу кибератаки, неразрешен достъп или кражба на модел. Тази защита може да бъде улеснена чрез осигуряване на тегла на моделите, алгоритми, сървъри и набори от данни, например чрез оперативни мерки за информационна сигурност, специфични политики за киберсигурност, подходящи технически и изпитани решения и контрол на кибердостъпа и физическия достъп, съобразени със съответните обстоятелства и рискове.
- (116) Службата по ИИ следва да насърчава и улеснява изготвянето, прегледа и адаптирането на кодекси за добри практики, като взема предвид международните подходи. Всички доставчици на модели на ИИ с общо предназначение биха могли да бъдат поканени да участват. За да се гарантира, че кодексите за добри практики отразяват съвременните технически постижения и са надлежно съобразени с набор от различни гледни точки, Службата по ИИ следва да си сътрудничи със съответните национални компетентни органи и би могла, когато е целесъобразно, да се консултира с организации на гражданското общество и други съответни заинтересовани страни и експерти, включително експертната група, за изготвянето на такива кодекси. Кодексите за добри практики следва да включват задълженията на доставчиците на модели на ИИ с общо предназначение и на модели на ИИ с общо предназначение, пораждащи системен риск. Освен това, по отношение на системните рискове, кодексите за добри практики следва да спомогнат за установяването на таксономия на вида и естеството на системните рискове на равнището на Съюза, включително техните източници. Кодексите за добри практики следва също така да бъдат съсредоточени върху конкретни мерки за оценка и ограничаване на риска.
- (117) Кодексите за добри практики следва да представляват основен инструмент за правилното спазване на задълженията, предвидени в настоящия регламент за доставчиците на модели на ИИ с общо предназначение. Доставчиците следва да могат да се основават на кодекси за добри практики, за да докажат спазването на задълженията. Комисията може да реши да одобри чрез акт за изпълнение кодекс за добри практики и да осигури общата му приложимост в рамките на Съюза или, като друга възможност, да предвиди общи правила за изпълнението на съответните задължения, ако до началото на прилагането на настоящия регламент даден кодекс за добри практики не може да бъде подготвен или не се счита за подходящ от Службата по ИИ. След като даден хармонизиран стандарт бъде публикуван и оценен като

подходящ за покриване на съответните задължения от Службата по ИИ, съответствието с европейски хармонизиран стандарт следва да дава на доставчиците презумпция за съответствие. Освен това доставчиците на модели на ИИ с общо предназначение следва да могат да докажат съответствие, като използват други подходящи средства, ако няма кодекси за добри практики или хармонизирани стандарти или ако решат да не разчитат на тях.

- (118) С настоящия регламент се уреждат системите с ИИ и моделите на ИИ, като се налагат определени изисквания и задължения за съответните пазарни участници, които ги пускат на пазара, пускат в действие или използват в Съюза, като по този начин се допълват задълженията на доставчиците на посреднически услуги, които интегрират такива системи или модели в своите услуги, които се уреждат от Регламент (ЕС) 2022/2065. Доколкото тези системи или модели са вградени в определени много големи онлайн платформи или много големи онлайн търсачки, за тях се прилага рамката за управление на риска, предвидена в Регламент (ЕС) 2022/2065. Следователно съответните задължения съгласно настоящия регламент следва да се считат за изпълнени, освен ако в такива модели не възникнат и се установят значителни системни рискове, които не са обхванати от Регламент (ЕС) 2022/2065. В тази контекст от доставчиците на много големи онлайн платформи и много големи онлайн търсачки се изисква да оценяват потенциалните системни рискове, произтичащи от проектирането, функционирането и използването на техните услуги, включително начина, по който проектирането на алгоритмични системи, използвани в услугата, може да допринесе за появата на такива рискове, както и системните рискове, произтичащи от евентуална неправилна експлоатация. Тези доставчици са длъжни също така да предприемат подходящи мерки за ограничаване при спазване на основните права.
- (119) Предвид бързия темп на иновациите и технологичното развитие на цифровите услуги, попадащи в обхвата на различните инструменти на правото на Съюза, по-специално като се има предвид използването и възприемането им от страна на техните получатели, системите с ИИ, които са предмет на настоящия регламент, могат да бъдат предоставяни като посреднически услуги или части от тях по смисъла на Регламент (ЕС) 2022/2065, който следва да се тълкува по технологично неутрален начин. Например системите с ИИ могат да се използват за предоставяне на онлайн търсачки, по-специално доколкото дадена система с ИИ, като например онлайн чатбот, извършва търсене по принцип на всички уебсайтове, след това интегрира резултатите в съществуващите си знания и използва актуализираните знания, за да генерира единен резултат, който съчетава различни източници на информация.
- (120) Освен това задълженията, наложени с настоящия регламент на доставчиците и внедрителите на някои системи с ИИ с цел откриване и оповестяване, че резултатите от тези системи са изкуствено генерирани или обработени, са от особено значение с оглед на ефективното прилагане на Регламент (ЕС) 2022/2065. Това се отнася по-специално за задълженията на доставчиците на много големи онлайн платформи или много големи онлайн търсачки да установяват и ограничават системните рискове, които могат да възникнат поради разпространението на съдържание, което е било изкуствено генерирано или обработено, и по-специално риска от действителни или предвидими отрицателни последици за демократичните процеси, гражданския дебат и изборните процеси, включително чрез дезинформация.
- (121) Стандартизацията следва да заема ключово място за осигуряването на технически решения на доставчиците, за да се гарантира спазването на настоящия регламент, съобразно съвременните технически постижения, с цел да се насърчат иновациите, както и конкурентоспособността и растежът на единния пазар. Съответствието с хармонизираните стандарти по смисъла на определението в член 2, точка 1, буква в) от Регламент (ЕС) № 1025/2012 на Европейския парламент и на Съвета⁽⁴¹⁾, които обикновено се очаква да отразяват съвременните технически постижения, следва да бъде средство за доказване на спазването на изискванията на настоящия регламент от доставчиците. Поради това следва да се насърчава балансирано представителство на интереси с участието в разработването на стандарти на всички съответни заинтересовани страни, по-специално МСП, организации на потребители и представляващите екологични и социални интереси заинтересовани страни в съответствие с членове 5 и 6 от Регламент (ЕС) № 1025/2012. За да се улесни съответствието, исканията за стандартизация следва да се отправят от Комисията без ненужно забавяне. При изготвянето на искането за стандартизация Комисията следва да се консултира с консултативния форум и със Съвета по ИИ, за да събере съответния експертен опит. При липсата на съответни позовавания на хармонизирани стандарти обаче Комисията следва да може да установява, чрез актове за изпълнение и след консултация с консултативния форум, общи спецификации за някои изисквания съгласно настоящия регламент. Общата спецификация следва да бъде извънредно алтернативно решение, за да се улесни изпълнението на задължението на доставчика да спазва изискванията на настоящия регламент, когато искането за стандартизация не е било прието от някоя от европейските организации за стандартизация или когато съответните хармонизирани стандарти не отразяват в достатъчна степен опасенията, свързани с основните права, или когато хармонизираните стандарти не отговарят на искането, или когато има забавяне в приемането на подходящ хармонизиран стандарт. Когато това забавяне в приемането на хармонизиран стандарт се дължи на техническата сложност на стандарта, това

⁽⁴¹⁾ 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).

следва да се вземе предвид от Комисията, преди да се разгледа възможността за установяване на общи спецификации. При разработването на общи спецификации Комисията се насърчава да си сътрудничи с международни партньори и международни органи за стандартизация.

- (122) Без да се засяга използването на хармонизирани стандарти и общи спецификации, е целесъобразно да се счита, че доставчиците на високорискова система с ИИ, която е била обучена и изпитана въз основа на данни, отразяващи конкретната географска, контекстуална, поведенческа или функционална среда, в която системата с ИИ е предназначена да бъде използвана, съответстват на съответната мярка, предвидена съгласно изискването за администриране на данни, определено в настоящия регламент. Без да се засягат изискванията, свързани с надеждността и точността, установени в настоящия регламент, в съответствие с член 54, параграф 3 от Регламент (ЕС) 2019/881 високорисковите системи с ИИ, които са сертифицирани или за които е издадена декларация за съответствие по схема за киберсигурност съгласно посочения регламент и данните за които са били публикувани в *Официален вестник на Европейския съюз*, следва да се считат за съответстващи на изискването за киберсигурност съгласно настоящия регламент, доколкото сертификатът за киберсигурност или декларацията за съответствие, или части от тях включват изискването за киберсигурност съгласно настоящия регламент. Това не засяга доброволния характер на тази схема за киберсигурност.
- (123) 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 пускането им в действие.
- (124) 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 въз основа на новата законодателна рамка, е целесъобразно съответствието на тези системи с ИИ с изискванията на настоящия регламент да се оценява като част от оценяването на съответствието, което вече е предвидено съгласно посоченото право. Следователно приложимостта на изискванията на настоящия регламент не следва да засяга специфичната логика, методика или обща структура за оценяване на съответствието съгласно съответното законодателство на Съюза за хармонизация.
- (125) С оглед на сложността на високорисковите системи с ИИ и свързаните с тях рискове, е важно да се разработи подходяща процедура за оценяване на съответствието за високорискови системи с ИИ, включваща нотифицирани органи, т.нар. оценяване на съответствието от трето лице. Като се има предвид обаче настоящият опит в областта на безопасността на продуктите на професионалните сертифициращи органи преди пускането на пазара, както и 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 трето лице 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, като единствено изключение са системите с ИИ, предназначени да се използват за биометрични цели.
- (126) С цел извършване на оценяване на съответствието от трето лице, когато това се изисква, националните компетентни органи следва да нотифицират 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 и на подходящи изисквания за киберсигурност. Националните компетентни органи следва да изпращат нотификацията за тези органи до Комисията и другите държави членки чрез средството за електронно нотифициране, разработено и управлявано от Комисията съгласно член R23 от приложение I към Решение № 768/2008/ЕО.
- (127) В съответствие с ангажиментите на Съюза съгласно Споразумението на Световната търговска организация за техническите пречки пред търговията е целесъобразно да се улесни взаимното признаване на резултатите от оценяването на съответствието, получени от компетентни органи за оценяване на съответствието, независимо от територията, на която са създадени, при условие че тези органи за оценяване на съответствието, създадени съгласно правото на трета държава, отговарят на приложимите изисквания на настоящия регламент и че Съюзът е сключил споразумение в това отношение. В този контекст Комисията следва активно да проучи възможните международни инструменти за тази цел и по-специално да се стреми към сключване на споразумения за взаимно признаване с трети държави.
- (128) В съответствие с общоприетото понятие за съществено изменение за продукти, регулирани от законодателството на Съюза за хармонизация, е целесъобразно дадена система с ИИ да се счита за нова система с ИИ, която следва да бъде подложена на ново оценяване на съответствието всеки път, когато настъпи промяна, която може да засегне съответствието на високорискова система с ИИ с настоящия регламент (например промяна на операционната система или на софтуерната архитектура), или когато предназначението на системата се промени. Въпреки това промените на алгоритъма или на действието на системи с ИИ, които продължават да се обучават след пускането им на пазара или пускането им в действие, а именно автоматично адаптират начина, по който се изпълняват функциите, не следва да се смятат за съществено изменение, при условие че тези промени са били предварително определени от доставчика и оценени към момента на оценяването на съответствието.

- (129) Високорисковите системи с ИИ следва да носят маркировката „СЕ“, указваща тяхното съответствие с настоящия регламент с цел свободно движение в рамките на вътрешния пазар. За високорисковите системи с ИИ, вградени в продукт, следва да се постави физическа маркировка „СЕ“, която може да бъде допълнена с цифрова маркировка „СЕ“. За високорисковите системи с ИИ, предоставяни само в цифров вид, следва да се използва цифрова маркировка „СЕ“. Държавите членки не следва да създават необосновани пречки пред пускането на пазара или пускането в действие на високорискови системи с ИИ, които съответстват на изискванията, предвидени в настоящия регламент, и носят маркировката „СЕ“.
- (130) При определени условия бързото осигуряване на иновативни технологии може да бъде от решаващо значение за здравето и безопасността на хората, опазването на околната среда и изменението на климата, както и за обществото като цяло. Поради това е целесъобразно по извънредни причини, свързани с обществената сигурност или защитата на живота и здравето на физическите лица, опазването на околната среда и защитата на ключови промишлени и инфраструктурни активи, органите за надзор на пазара да могат да разрешават пускането на пазара или пускането в действие на системи с ИИ, които не са преминали оценяване на съответствието. В надлежно обосновани случаи, предвидени в настоящия регламент, правоохранителните органи или органите за гражданска защита могат да пуснат в действие конкретна високорискова система с ИИ без разрешението на органа за надзор на пазара, при условие че такова разрешение е поискано без ненужно забавяне по време на използването или след него.
- (131) С цел да се улесни работата на Комисията и на държавите членки в областта на ИИ, 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, както и от доставчиците, които считат, че дадена система с ИИ, включена в случаите на високорискова употреба, посочени в приложение към настоящия регламент, не е високорискова въз основа на дерогация, следва да се изисква да се регистрират и да впишат информацията за своята система с ИИ в база данни на ЕС, която да бъде създадена и управлявана от Комисията. Преди да използват такава система с ИИ, включена в случаите на високорискова употреба в приложение към настоящия регламент, внедрителите на високорискови системи с ИИ, които са публични органи, агенции или структури, следва да се регистрират в тази база данни и да изберат системата, която възнамеряват да използват. Останалите внедрители следва да имат право да направят това на доброволна основа. Този раздел на базата данни на ЕС следва да бъде публично достъпен, безплатен, а информацията следва да бъде лесна за навигация, разбираема и машинночетима. Базата данни на ЕС следва също така да бъде лесна за ползване, например като осигурява функции за търсене, включително чрез ключови думи, за да се даде възможност на широката общественост да намери съответната информация, която трябва да бъде предоставена при регистрацията на високорискови системи с ИИ, както и информация за случаите на употреба на високорисковите системи с ИИ, посочени в приложение към настоящия регламент, на които отговарят високорисковите системи с ИИ. Всяко съществено изменение на високорискови системи с ИИ също следва да се регистрира в базата данни на ЕС. За високорисковите системи с ИИ в правоохранителната област и в областта на управлението на миграцията, убежището и граничния контрол задълженията за регистрация следва да се изпълняват в защитен непубличен раздел на базата данни на ЕС. Достъпът до защитения непубличен раздел следва да бъде строго ограничен до Комисията, както и до органите за надзор на пазара по отношение на техния национален раздел на тази база данни. Високорисковите системи с ИИ в областта на критичната инфраструктура следва да се регистрират само на национално равнище. Комисията следва да бъде администратор на базата данни на ЕС в съответствие с Регламент (ЕС) 2018/1725. За да се гарантира цялостна готовност на базата данни при нейното въвеждане, процедурата по създаване на базата данни на ЕС следва да включва разработването на функционални спецификации от Комисията и независим одитен доклад. Комисията следва да вземе предвид рисковете, свързани с киберсигурността, когато изпълнява задачите си като администратор на данни по отношение на базата данни на ЕС. За да се увеличи максимално достъпността и използването на базата данни на ЕС от обществеността, базата данни на ЕС, включително информацията, предоставяна чрез нея, следва да отговаря на изискванията на Директива (ЕС) 2019/882.
- (132) Някои системи с ИИ, предназначени да взаимодействат с физически лица или да генерират съдържание, могат да породят особени рискове от измама на основата на прилика или заблуда, независимо дали отговарят на критериите за високорискови системи, или не. Поради това при определени обстоятелства при използването на тези системи следва да се прилагат специални задължения за прозрачност, без да се засягат изискванията и задълженията за високорискови системи с ИИ и при прилагане на целеви изключения с цел да се вземат предвид особените правоохранителни нужди. По-специално, физическите лица следва да бъдат уведомявани, че взаимодействат със система с ИИ, освен ако това не е очевидно от гледна точка на физическо лице, което е в разумни граници осведомено, наблюдателно и съобразително предвид обстоятелствата и контекста на използване. При изпълнението на това задължение следва да се вземат предвид характеристиките на физическите лица, принадлежащи към уязвими групи поради своята възраст или увреждане, доколкото системата с ИИ е предназначена да взаимодейства и с тези групи. Наред с това, физическите лица следва да бъдат уведомявани, когато са изложени на системи с ИИ, които чрез обработване на биометричните им данни могат да определят или да направят изводи за емоциите или намеренията на тези лица или да ги отнесат към конкретни категории. Подобни конкретни категории може да са свързани с аспекти като пол, възраст, цвят на косата, цвят на очите, татуировки, личностни черти, етнически произход, лични предпочитания и интереси. Тази информация и уведомленията следва да се предоставят в достъпни формати за хората с увреждания.

- (133) Различни системи с ИИ могат да генерират големи количества синтетично съдържание, което хората все по-трудно могат да разграничават от генерирано от човека и автентично съдържание. Широката наличност и нарастващият капацитет на тези системи оказват значително влияние върху почтеността и доверието в информационната екосистема, което поражда нови рискове от масивно навлизане на невярна информация и манипулиране, измами на основата на прилика и заблуда на потребителите. С оглед на това въздействие, бързия темп на развитие на технологиите и необходимостта от нови методи и техники за проследяване на произхода на информацията е целесъобразно да се изисква от доставчиците на тези системи да въграждат технически решения, позволяващи маркиране в машинночитим формат и разпознаване, че резултатът е генериран или обработен от система с ИИ, а не от човек. Тези техники и методи следва да бъдат достатъчно надеждни, оперативно съвместими, ефективни и сигурни, доколкото това е технически осъществимо, и да се основават на наличните техники или на комбинация от такива техники, например водни знаци, идентифициране на метаданни, криптографски методи за доказване на произхода и автентичността на съдържанието, методи за регистриране, пръстови отпечатъци или други техники, в зависимост от случая. При изпълнението на това задължение доставчиците следва също така да отчитат особеностите и ограниченията на различните видове съдържание и технологичното и пазарното развитие в тази област, които намират отражение в общопризнатото най-съвременно равнище на технологиите. Тези техники и методи могат да бъдат приложени на равнището на системата с ИИ или на равнището на модела на ИИ, включително при модели на ИИ с общо предназначение, генериращи съдържание, като по този начин се улеснява изпълнението на това задължение от доставчика надолу по веригата на системата с ИИ. За да бъде пропорционално това задължение за маркиране, е целесъобразно да се предвиди то да няма приложение при системи с ИИ, изпълняващи предимно помощна функция при стандартно редактиране, или за системи с ИИ, които не променят съществено входящите данни, въведени от внедрителя, или тяхната семантика.
- (134) Освен техническите решения, приложени от доставчиците на системата с ИИ, и внедрителите, които използват система с ИИ за генериране или обработване на изображения, аудио или видео съдържание, наподобяващи до голяма степен съществуващи лица, предмети, места, субекти или събития, които е вероятно някой да приеме за истински или достоверни (т.нар. „убедителни фалшификати“), следва също по ясен и разпознаваем начин да оповестят обстоятелството, че съдържанието е било изкуствено генерирано или обработено, като обозначат по подходящ начин продукта от работата на ИИ и разкрият неговия изкуствен произход. Спазването на това задължение за прозрачност не следва да се тълкува в смисъл, че използването на системата с ИИ или резултатите от нея възпрепятства правото на свобода на изразяване на мнение и правото на свобода на изкуствата и науките, гарантирани от Хартата, по-специално когато съдържанието е част от произведение или програма, които имат очевиден творчески, сатиричен, артистичен, художествен или подобен характер, при прилагане на подходящи гаранции за правата и свободите на трети лица. В тези случаи задължението за прозрачност по отношение на убедителните фалшификати, предвидено в настоящия регламент, се ограничава до оповестяване на наличието на такова генерирано или обработено съдържание по подходящ начин, който не възпрепятства показването или използването на произведението, включително нормалната му експлоатация и употреба, като същевременно се запазват полезността и качеството на произведението. Освен това е целесъобразно да се предвиди подобно задължение за оповестяване във връзка с текст, който е генериран или обработен от ИИ, доколкото той е публикуван с цел информиране на обществеността по въпроси от обществен интерес, освен ако генерираното от ИИ съдържание не е преминало преглед от човек или подложено на редакторски контрол и редакционната отговорност за публикуването му се носи от физическо или юридическо лице.
- (135) Без да се засягат задължителният характер и пълната приложимост на задълженията за прозрачност, Комисията може също да насърчава и улеснява изготвянето на кодекси за добри практики на равнището на Съюза с цел да се допринесе за ефективното изпълнение на задълженията за откриване и обозначаване на изкуствено генерирано или обработено съдържание, включително да се съдейства във връзка с практически правила, които да осигурят при необходимост достъпност на механизмите за откриване и да подпомагат сътрудничеството с други участници по веригата за създаване на стойност, разпространение на съдържание или проверка на неговата автентичност и произход, за да се даде възможност на обществеността действително да разпознава генерираното от ИИ съдържание.
- (136) Задълженията, наложени в настоящия регламент на доставчиците и внедрителите на някои системи с ИИ с цел откриване и обозначаване, че резултатите от тези системи са изкуствено генерирани или обработени, са от особено значение с оглед на ефективното прилагане на Регламент (ЕС) 2022/2065. Това се отнася по-специално за задълженията на доставчиците на много големи онлайн платформи или много големи онлайн търсачки да установяват и ограничават системните рискове, които могат да възникнат поради разпространението на съдържание, което е било изкуствено генерирано или обработено, и по-специално риска от действителни или предвидими отрицателни последици за демократичните процеси, гражданския дебат и изборните процеси, включително чрез дезинформация. Изискването съгласно настоящия регламент за обозначаване на съдържание, генерирано от системи с ИИ, не засяга задължението по член 16, параграф 6 от Регламент (ЕС) 2022/2065 на доставчиците на хостинг услуги да обработват уведомления за незаконно съдържание, получени съгласно член 16, параграф 1 от посочения регламент, и не следва да влияе на оценката и решението относно незаконния характер на конкретното съдържание. Тази преценка следва да се извършва единствено с оглед на правилата, уреждащи законосъобразността на съдържанието.

- (137) Спазването на задълженията за прозрачност относно системите с ИИ, обхванати от настоящия регламент, не следва да се тълкува като знак, че използването на системата с ИИ или на резултатите от нея е законосъобразно съгласно настоящия регламент или друго законодателство на Съюза и на държава членка, и не следва да засяга други задължения за прозрачност за внедрители на системи с ИИ, предвидени в правото на Съюза или в националното право.
- (138) ИИ е бързо развиваща се съвкупност от технологии, която изисква регулаторен надзор и безопасно и контролирано пространство за експериментирание, като същевременно се гарантира отговорното новаторство и интегрирането на подходящи предпазни мерки и мерки за ограничаване на риска. За да се гарантира благоприятна за иновациите, ориентирана към бъдещето и устойчива на смущения правна рамка, държавите членки следва да гарантират, че националните им компетентни органи създават най-малко една регулаторна лаборатория в областта на ИИ на национално равнище, 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 пуснати в действие по друг начин. Държавите членки биха могли да изпълнят това задължение и чрез участие във вече съществуващи регулаторни лаборатории или съвместно създаване на лаборатория с компетентните органи на една или повече държави членки, доколкото това участие осигурява равностойно национално покритие за участващите държави членки. Регулаторните лаборатории в областта на ИИ могат да бъдат създадени във физическа, цифрова или хибридна форма и да включват както физически, така и цифрови продукти. Създаващите ги органи следва също така да гарантират, че регулаторните лаборатории в областта на ИИ разполагат с подходящи ресурси за функционирането си, включително финансови и човешки ресурси.
- (139) Целите на регулаторните лаборатории в областта на ИИ 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 друго съответно право на Съюза и национално право. В допълнение регулаторните лаборатории в областта на ИИ следва да имат за цел подобряване на правната сигурност за новаторите и надзора и разбирането от страна на компетентните органи на възможностите, нововъзникващите рискове и въздействието на използването на ИИ, улесняване на натрупването на регулаторен опит от страна на органите и предприятията, включително с оглед на бъдещи изменения на правната рамка, подкрепа за сътрудничеството и обмена на най-добри практики с органите, участващи в регулаторната лаборатория в областта на ИИ, както и ускоряване на достъпа до пазарите, включително чрез премахване на пречките пред МСП, включително новосъздадените предприятия. Следва да се предостави широк достъп до регулаторните лаборатории в областта на ИИ на територията на Съюза, като се обърне специално внимание на достъпността им за МСП, включително новосъздадените предприятия. Участието в регулаторните лаборатории в областта на ИИ следва да е насочено към въпроси, които поражда правна несигурност за доставчиците и потенциалните доставчици при въвеждането на иновации и експериментирането с ИИ в Съюза и да допринася за основан на факти регулаторен опит. Поради това надзорът върху системите с ИИ в регулаторните лаборатории в областта на ИИ следва да обхваща тяхното разработване, обучение, изпитване и валидиране, преди системите да бъдат пуснати на пазара или пуснати в действие, както и концепцията за и настъпването на съществено изменение, което може да изисква провеждането на нова процедура за оценяване на съответствието. Всички значителни рискове, установени по време на разработването и изпитването на такива системи с ИИ, следва да водят до адекватни ограничителни мерки, а при липса на такива — до спиране на процеса на разработване и изпитване. Когато е целесъобразно, националните компетентни органи, които създават регулаторни лаборатории в областта на ИИ, следва да си сътрудничат с други съответни органи, включително упражняващите надзор върху защитата на основните права, и биха могли да позволят привличането на други участници в екосистемата на ИИ, като например национални или европейски организации за стандартизация, нотифицирани органи, структури за изпитване и експериментирание, лаборатории за научни изследвания и експерименти, европейски цифрови иновационни центрове и съответни заинтересовани страни и организации на гражданското общество. За да се гарантират еднакво прилагане в целия Съюз и икономии на мащаб, е целесъобразно да се установят общи правила за създаването на регулаторните лаборатории в областта на ИИ и рамка за сътрудничество между съответните органи, участващи в надзора на лабораториите. Регулаторните лаборатории в областта на ИИ, създадени съгласно настоящия регламент, не следва да засягат друго право, допускащо създаването на други лаборатории и чиято цел е да се гарантира спазването на правни норми извън настоящия регламент. Когато е целесъобразно, съответните компетентни органи, които отговарят за други регулаторни лаборатории, следва да преценят доколко би било полезно използването им и с цел осигуряване на съответствието на системите с ИИ с настоящия регламент. По споразумение между националните компетентни органи и участниците в регулаторната лаборатория в областта на ИИ в такава лаборатория също така може да се извършва изпитване в реални условия и върху него да се осъществява надзор.
- (140) В съответствие с член 6, параграф 4 и член 9, параграф 2, буква ж) от Регламент (ЕС) 2016/679 и членове 5, 6 и 10 от Регламент (ЕС) 2018/1725 и без да се засягат член 4, параграф 2 и член 10 от Директива (ЕС) 2016/680, настоящият регламент следва да предостави на доставчиците и потенциалните доставчици в регулаторните лаборатории в областта на ИИ правното основание за използването, само при определени условия, на лични данни, събирани за други цели, с оглед на разработването на определени системи с ИИ в обществен интерес в рамките на регулаторната лаборатория в областта на ИИ. Всички други задължения на администраторите на данни и правата на субектите на данни съгласно регламенти (ЕС) 2016/679 и (ЕС) 2018/1725 и Директива (ЕС) 2016/680 остават приложими. По-специално настоящият регламент не следва да предоставя правно основание по смисъла на член 22, параграф 2, буква б) от Регламент (ЕС) 2016/679 и член 24, параграф 2, буква б) от Регламент (ЕС) 2018/1725. Доставчиците и потенциалните доставчици в регулаторната лаборатория в областта на ИИ следва да осигурят подходящи гаранции и да си сътрудничат с компетентните органи, включително като следват техните насоки и действат бързо

и добросъвестно, за да ограничат по подходящ начин всички установени значителни рискове за безопасността, здравето и основните права, които могат да се проявят по време на разработването, изпитването и експериментирането в лабораторията.

- (141) За да се ускори процесът на разработване и пускане на пазара на високорисковите системи с ИИ, чийто списък се съдържа в приложение към настоящия регламент, е важно доставчиците или потенциалните доставчици на такива системи да могат да ползват специален режим за изпитване на тези системи в реални условия и без да участват в регулаторна лаборатория в областта на ИИ. В такива случаи обаче, предвид евентуалните последици, които това изпитване може да има върху хората, следва да се гарантира, че настоящият регламент въвежда подходящи и достатъчни гаранции и условия по отношение на доставчиците или потенциалните доставчици. Тези гаранции следва да включват, наред с другото, искането на информирано съгласие от физическите лица за участие в изпитвания в реални условия, освен в правоохранителната област, когато искането на информирано съгласие би попречило на изпитването на системата с ИИ. Съгласието на субектите на данни да участват в такива изпитвания в съответствие с настоящия регламент е различно от съгласието на субектите на данни личните им данни да бъдат обработвани съгласно съответното законодателство за защита на данните и не засяга това съгласие. Важно е също така рисковете да бъдат сведени до минимум и компетентните органи да могат да упражняват надзор, във връзка с което да се въведат изисквания потенциалните доставчици да представят на компетентния орган за надзор на пазара план за изпитване в реални условия, да регистрират изпитването в специални раздели на базата данни на ЕС с ограничен брой изключения, да определят ограничения на срока, в който може да се извърши изпитването, както и да се изискват допълнителни гаранции за лица, принадлежащи към определени уязвими групи, и писмено споразумение, в което се установяват функциите и отговорностите на потенциалните доставчици и внедрителите и ефективен надзор от страна на компетентния персонал, участващ в изпитванията в реални условия. Освен това е целесъобразно да се предвидят допълнителни гаранции, за да се гарантира, че прогнозите, препоръките или решенията на дадена система с ИИ могат ефективно да се отменят и пренебрегнат, както и че личните данни са защитени и се заличават, след като субектите в изпитването са оттеглили съгласието си за участие в изпитването, без да се засягат правата им като субекти на данни съгласно правото на Съюза в областта на защитата на данните. По отношение на предаването на данни е целесъобразно също така да се предвиди, че данните, събирани и обработвани за целите на изпитването в реални условия, следва да се предават на трети държави само при прилагане на подходящи и приложими гаранции съгласно правото на Съюза, по-специално в съответствие с основанията за предаване на лични данни съгласно правото на Съюза относно защитата на данните, докато по отношение на неличните данни се прилагат подходящи гаранции в съответствие с правото на Съюза, като например регламенти (ЕС) 2022/868⁽⁴²⁾ и (ЕС) 2023/2854⁽⁴³⁾ на Европейския парламент и на Съвета.
- (142) За да се гарантира, че ИИ води до благоприятни за обществото и околната среда резултати, държавите членки се насърчават да подкрепят и поощряват научните изследвания и разработването на решения в областта на ИИ, способстващи за постигането на такива резултати — например основани на ИИ решения за увеличаване на достъпността за хората с увреждания, противодействие на социално-икономическите неравенства или постигане на екологичните цели, чрез разпределяне на достатъчно ресурси, включително публично финансиране и финансиране от Съюза, и когато е целесъобразно и при условие че са изпълнени критериите за допустимост и подбор, разглеждане на проекти, които преследват тези цели. Такива проекти следва да се основават на принципа на интердисциплинарното сътрудничество между разработчици на ИИ, експерти по въпросите на неравенството и недискриминацията, достъпността, правата на потребителите, правата, свързани с околната среда, и цифровите права, както и академичните среди.
- (143) С цел насърчаване и защита на иновациите е важно да се обърне специално внимание на интересите на МСП, включително новосъздадените предприятия, които са доставчици или внедрители 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. Държавите членки следва да осигуряват на МСП, включително новосъздадените предприятия, които имат седалище или клон в Съюза, приоритетен достъп до регулаторните лаборатории в областта на ИИ, при условие че те отговарят на условията за допустимост и на критериите за подбор, без да се възпрепятства достъпът на други доставчици и потенциални доставчици до лабораториите, при условие че са изпълнени същите условия и критерии. Държавите членки следва да използват наличните, а когато е целесъобразно — да създават нови, специални канали за комуникация с МСП, новосъздадени предприятия, внедрители, други новатори и — в зависимост от случая — органи на местна власт, с цел да подпомагат МСП по пътя им на развитие чрез даване на насоки и отговаряне на запитвания във връзка с прилагането на настоящия регламент. Когато е целесъобразно, тези канали следва да работят заедно, за да се създадат полезни взаимодействия и да се гарантира еднообразност на насоките за МСП, включително новосъздадените предприятия, и внедрителите. Наред с това държавите членки следва да улесняват участието на МСП и на други заинтересовани страни в процесите на разработване на стандарти. Освен това, при определянето на таксите за оценяване на съответствието нотифицираните органи следва да вземат предвид

⁽⁴²⁾ Регламент (ЕС) 2022/868 на Европейския парламент и на Съвета от 30 май 2022 г. относно европейска рамка за управление на данните и за изменение на Регламент (ЕС) 2018/1724 (Акт за управление на данните) (ОВ L 152, 3.6.2022 г., стр. 1).

⁽⁴³⁾ Регламент (ЕС) 2023/2854 на Европейския парламент и на Съвета от 13 декември 2023 г. относно хармонизирани правила за справедлив достъп до данни и за тяхното използване и за изменение на Регламент (ЕС) 2017/2394 и Директива (ЕС) 2020/1828 (Акт за данните) (ОВ L, 2023/2854, 22.12.2023, ELI: <http://data.europa.eu/eli/reg/2023/2854/oj>).

особените интереси и нужди на доставчиците, които са МСП, включително новосъздадени предприятия. Комисията следва да оценява редовно разходите на МСП, включително новосъздадените предприятия, за сертифициране и привеждане в съответствие чрез прозрачни консултации и следва да работи с държавите членки за понижаването на тези разходи. Така например разходите за превод, свързани със задължителната документация и комуникацията с органите, могат да представляват значителни разходи за доставчиците и другите оператори, по-специално за по-малките. Държавите членки следва по възможност да гарантират, че един от езиките, 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 внедрители. За да се отговори на специфичните нужди на МСП, включително новосъздадените предприятия, Комисията следва да осигури стандартизирани образци за областите, обхванати от настоящия регламент, по искане на Съвета по ИИ. Освен това Комисията следва да допълни усилията на държавите членки, като осигури единна информационна платформа с лесна за ползване информация относно настоящия регламент, предназначена за всички доставчици и внедрители, като организира подходящи комуникационни кампании за повишаване на осведомеността относно задълженията, произтичащи от настоящия регламент, и като оценява и насърчава сближаването на най-добрите практики, прилагани в рамките на процедурите за възлагане на обществени поръчки във връзка със системите с ИИ. Средните предприятия, които доскоро са съответствали на критериите за малки предприятия по смисъла на приложението към Препоръка 2003/361/ЕО на Комисията⁽⁴⁴⁾, следва да имат достъп до тези мерки за подкрепа, тъй като е възможно тези нови средни предприятия да не разполагат с правните ресурси и обучението, необходими, за да се гарантира правилното разбиране и спазване на настоящия регламент.

- (144) С цел насърчаване и защита на иновациите платформата за ИИ по заявка, всички съответни програми и проекти на Съюза за финансиране, като например програмите „Цифрова Европа“ и „Хоризонт Европа“, изпълнявани от Комисията и държавите членки на национално равнище или на равнището на Съюза, следва, когато е целесъобразно, да допринасят за постигането на целите на настоящия регламент.
- (145) За да се сведат до минимум рисковете за правоприлагането, произтичащи от липсата на знания и експертен опит на пазара, както и за да се улесни спазването на задълженията по настоящия регламент от страна на доставчиците, по-специално МСП, включително новосъздадените предприятия, и нотифицираните органи, платформата за ИИ по заявка, европейските цифрови иновационни центрове и структурите за изпитване и експериментиране, създадени от Комисията и държавите членки на национално равнище или на равнището на Съюза, следва да допринасят за прилагането на настоящия регламент. В рамките на своята мисия и области на компетентност платформата за ИИ по заявка, европейските цифрови иновационни центрове и структурите за изпитване и експериментиране могат да предоставят по-специално техническа и научна подкрепа на доставчиците и нотифицираните органи.
- (146) Освен това, предвид твърде малкия размер на някои оператори и с цел да се гарантира пропорционалност по отношение на разходите за иновации, е целесъобразно да се даде възможност на микропредприятията да изпълнят едно от най-скъпо струващите задължения, а именно създаването на система за управление на качеството, по опростен начин, което би намалило административната тежест и разходите за тези предприятия, без да се засягат равнището на защита и необходимостта от съответствие с изискванията за високорисковите системи с ИИ. Комисията следва да разработи насоки с цел да се определят елементите на системата за управление на качеството, които трябва да бъдат изпълнени по този опростен начин от микропредприятията.
- (147) Целесъобразно е Комисията да улеснява, доколкото е възможно, достъпа до структури за изпитване и експериментиране 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 регламенти (ЕС) 2017/745 и (ЕС) 2017/746.
- (148) С настоящия регламент следва да се създаде рамка за управление, която да позволява координация и подкрепа при прилагането на настоящия регламент на национално равнище, както и изграждане на капацитет на равнището на Съюза и включване на заинтересованите страни в областта на изкуствения интелект. Ефективното изпълнение и прилагане на настоящия регламент изискват рамка за управление, която да дава възможност за координация и изграждане на експертен опит на централно ниво, на равнището на Съюза. Службата по ИИ беше създадена с решение на Комисията⁽⁴⁵⁾ с мисията да развива експертния опит и способностите на Съюза в областта на ИИ и да допринася за прилагането на правото на Съюза в областта на ИИ. Държавите членки следва да улесняват изпълнението на задачите на Службата по ИИ с цел да се подпомогне развитието на експертния опит на Съюза и на способностите на равнището на Съюза и да се укрепи функционирането на цифровия единен пазар. Наред с това следва да бъдат създадени Съвет по ИИ, съставен от представители на държавите членки, експертна група, с която да се привлече научната общност, и консултативен форум, чрез който заинтересованите страни да допринасят за прилагането на настоящия регламент както на национално равнище, така и на равнището на Съюза. Развитието на

⁽⁴⁴⁾ 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).

⁽⁴⁵⁾ Решение на Комисията от 24.1.2024 г. за създаване на Европейска служба по изкуствен интелект C (2024) 390.

експертния опит и способностите на Съюза следва да включва също така използването на съществуващите ресурси и експертен опит, по-специално чрез полезни взаимодействия със структури, изградени в контекста на прилагането в рамките на Съюза на друго законодателство, както и полезни взаимодействия със свързани инициативи на равнището на Съюза, например Съвместното предприятие за европейски високопроизводителни изчисления (EuroHPC) и съоръженията за изпитване и експериментирание с ИИ в рамките на програмата „Цифрова Европа“.

- (149) С цел подпомагане на безпрепятственото, ефективно и хармонизирано прилагане на настоящия регламент следва да бъде създаден Съвет по ИИ. Той следва да отразява различните интереси в рамките на екосистемата на ИИ и да се състои от представители на държавите членки. Съветът по ИИ следва да отговаря за изпълнението на редица консултативни задачи, включително да приема становища, препоръки, съвети или да допринася за приемането на насоки по въпроси, свързани с изпълнението на настоящия регламент, включително по въпроси на прилагането, техническите спецификации или съществуващите стандарти във връзка с изискванията, установени в настоящия регламент, и да консултира Комисията и държавите членки и техните национални компетентни органи по конкретни въпроси, свързани с ИИ. За да се осигури известна гъвкавост за държавите членки при определянето на техните представители в Съвета по ИИ, представители могат да бъдат всички лица, принадлежащи към публични субекти, които следва да разполагат със съответните компетентност и правомощия да улесняват координацията на национално равнище и да допринасят за изпълнението на задачите на Съвета по ИИ. Съветът по ИИ следва да създаде две постоянни подгрупи, които да осигуряват платформа за сътрудничество и обмен между органите за надзор на пазара и нотифициращите органи по въпроси, свързани съответно с надзора на пазара и нотифицираните органи. Постоянната подгрупа за надзор на пазара следва да действа като група за административно сътрудничество (ADCO група) за настоящия регламент по смисъла на член 30 от Регламент (ЕС) 2019/1020. В съответствие с член 33 от същия регламент Комисията следва да подпомага дейностите на постоянната подгрупа за надзор на пазара чрез извършване на оценки или проучвания на пазара, по-специално с цел да се установят аспекти на настоящия регламент, изискващи специфична и спешна координация между органите за надзор на пазара. Съветът по ИИ може да създаде други постоянни или временни подгрупи, когато това е целесъобразно за разглеждането на конкретни въпроси. Съветът по ИИ следва също така да си сътрудничи, когато е целесъобразно, със съответните органи, експертни групи и мрежи на Съюза, извършващи дейност в контекста на съответното право на Съюза, включително по-специално извършващите дейност съгласно правото на Съюза в областта на данните и цифровите продукти и услуги.
- (150) За да се гарантира участието на заинтересованите страни в изпълнението и прилагането на настоящия регламент, следва да се създаде консултативен форум, който да консултира и да предоставя технически експертни становища на Съвета по ИИ и на Комисията. За да се гарантира разнообразно и балансирано представителство на заинтересованите страни, свързани с търговски и нетърговски интереси и, в рамките на категорията на търговските интереси, на МСП и други предприятия, консултативният форум следва да включва, наред с другото, стопанския сектор, новосъздадените предприятия, МСП, академичните среди, гражданското общество, включително социалните партньори, както и Агенцията за основните права, ENISA, Европейския комитет по стандартизация (CEN), Европейския комитет за стандартизация в електротехниката (CENELEC) и Европейския институт за стандарти в далекосъобщенията (ETSI).
- (151) За да се подпомогне изпълнението и прилагането на настоящия регламент, и по-специално дейностите по мониторинг на Службата по ИИ по отношение на моделите на ИИ с общо предназначение, следва да се създаде експертна група, съставена от независими експерти. Независимите експерти, които влизат в състава на експертната група, следва да бъдат подбрани въз основа на актуални научни или технически експертни познания в областта на ИИ, да изпълняват задачите си безпристрастно и обективно и да гарантират поверителността на информацията и данните, получени при изпълнението на задачите и дейностите си. За да се даде възможност за укрепване на националния капацитет, необходим за ефективното прилагане на настоящия регламент, държавите членки следва да могат да искат съдействие от експертите, влизащи в състава на експертната група, във връзка с дейностите си по прилагане на регламента.
- (152) С цел да се допринесе за адекватното правоприлагане по отношение на системите с ИИ и да се укрепи капацитетът на държавите членки, следва да се създадат структури на Съюза за подкрепа на изпитванията в областта на ИИ, които да бъдат на разположение на държавите членки.
- (153) Държавите членки заемат ключово място в прилагането и изпълнението на настоящия регламент. Във връзка с това всяка държава членка следва да определи най-малко един нотифициращ орган и най-малко един орган за надзор на пазара в качеството им на национални компетентни органи за целите на надзора върху прилагането и изпълнението на настоящия регламент. Държавите членки могат да решат да определят всякакъв вид публичен субект да изпълнява задачите на националните компетентни органи по смисъла на настоящия регламент, в съответствие със своите конкретни национални организационни характеристики и нужди. С цел да се повиши ефективността на организацията от страна на държавите членки и да се създаде единно звено за контакт с обществеността и други партньори на равнището на държавите членки и на Съюза, всяка държава членка следва да определи орган за надзор на пазара, който да изпълнява функциите на единно звено за контакт.

- (154) Националните компетентни органи следва да упражняват правомощията си независимо, безпристрастно и непредубедено, за да бъдат спазени принципите за обективност в дейностите и задачите им и да се гарантира прилагането и изпълнението на настоящия регламент. Членовете на тези органи следва да се въздържат от всякакви действия, несъвместими с техните задължения, и да спазват правилата за поверителност съгласно настоящия регламент.
- (155) За да се гарантира, че доставчиците на високорискови системи с ИИ могат да вземат предвид опита от използването на високорискови системи с ИИ с цел да подобряват своите системи и процеса на проектиране и разработване, или че могат едновременно да предприемат евентуални коригиращи действия, всички доставчици следва да разполагат със система за мониторинг след пускането на пазара. Когато е целесъобразно, мониторингът след пускането на пазара следва да включва анализ на взаимодействието с други системи с ИИ, включително други устройства и софтуер. Мониторингът след пускането на пазара не следва да обхваща чувствителни оперативни данни на внедрители, които са правоохранителни органи. Тази система е от ключово значение и с оглед на това да се гарантира, че възможните рискове, произтичащи от системите с ИИ, които продължават да се обучават след пускането им на пазара или пускането им в действие, могат да бъдат преодоляни по-ефективно и своевременно. В този контекст от доставчиците следва също да се изисква да разполагат със система за докладване до съответните органи за всякакви сериозни инциденти, които произтичат от използването на техните системи с ИИ и представляват инцидент или неизправност, водещ(а) до смърт или сериозно увреждане на здравето, сериозно и необратимо нарушаване на управлението и експлоатацията на критична инфраструктура, нарушения на задължения съгласно правото на Съюза, имащо за цел да защитава основните права, или сериозно увреждане на имущество или на околната среда.
- (156) С оглед да се гарантира подходящо и ефективно прилагане на изискванията и задълженията, установени с настоящия регламент, който е част от законодателството на Съюза за хармонизация, системата за надзор на пазара и съответствие на продуктите, установена с Регламент (ЕС) 2019/1020, следва да се прилага в своята цялост. Органите за надзор на пазара, определени съгласно настоящия регламент, следва да разполагат с всички правомощия за осигуряване на спазването, установени съгласно настоящия регламент и Регламент (ЕС) 2019/1020, и следва да упражняват своите правомощия и да изпълняват своите задължения независимо, безпристрастно и непредубедено. Въпреки че за по-голямата част от системите с ИИ не се прилагат специални изисквания и задължения съгласно настоящия регламент, органите за надзор на пазара могат да предприемат мерки по отношение на всички системи с ИИ, когато те представляват риск в съответствие с настоящия регламент. Поради особеното естество на институциите, агенциите и органите на Съюза, попадащи в обхвата на настоящия регламент, е целесъобразно Европейският надзорен орган по защита на данните да бъде определен за компетентен орган за надзор на пазара по отношение на тях. Това не следва да засяга определянето на национални компетентни органи от държавите членки. Дейностите по надзор на пазара не следва да засягат способността на поднадзорните субекти да изпълняват задачите си по независим начин, когато тази независимост се изисква от правото на Съюза.
- (157) Настоящият регламент не засяга компетентността, задачите, правомощията и независимостта на съответните национални публични органи или структури, които упражняват надзор върху прилагането на правото на Съюза за защита на основните права, включително органите по въпросите на равенството и органите за защита на данните. Когато това е необходимо за упражняването на техните правомощия, тези национални публични органи или структури следва също така да имат достъп до всяка документация, изготвена съгласно настоящия регламент. Следва да се установи специална предпазна процедура, за да се гарантира адекватното и навременно осигуряване на спазването по отношение на системите с ИИ, които представляват риск за здравето, безопасността и основните права. Процедурата за такива системи с ИИ, представляващи риск, следва да се прилага за високорисковите системи с ИИ, представляващи риск, забранените системи, които са били пуснати на пазара, пуснати в действие или използвани в нарушение на определените в настоящия регламент забранени практики, и системите с ИИ, които са били предоставени в нарушение на установените в настоящия регламент изисквания за прозрачност и представляващи риск.
- (158) Правото на Съюза в областта на финансовите услуги включва правила и изисквания за вътрешно управление и управление на риска, 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 изпълнение и прилагане на задълженията по настоящия регламент и на съответните правила и изисквания съгласно правните актове на Съюза в областта на финансовите услуги, органите, компетентни за надзора и прилагането съгласно тези правни актове, и по-специално компетентните органи по смисъла на Регламент (ЕС) 575/2013 на Европейския парламент и на Съвета ⁽⁴⁶⁾ и директиви 2008/48/ЕО ⁽⁴⁷⁾, 2009/138/ЕО ⁽⁴⁸⁾, 2013/36/ЕС ⁽⁴⁹⁾, 2014/17/ЕС ⁽⁵⁰⁾ и (ЕС) 2016/97 ⁽⁵¹⁾ на

⁽⁴⁶⁾ Регламент (ЕС) № 575/2013 на Европейския парламент и на Съвета от 26 юни 2013 г. относно пруденциалните изисквания за кредитните институции и инвестиционните посредници и за изменение на Регламент (ЕС) № 648/2012 (ОВ L 176, 27.6.2013 г., стр. 1).

⁽⁴⁷⁾ Директива 2008/48/ЕО на Европейския парламент и на Съвета от 23 април 2008 г. относно договорите за потребителски кредити и за отмяна на Директива 87/102/ЕИО на Съвета (ОВ L 133, 22.5.2008 г., стр. 66).

⁽⁴⁸⁾ Директива 2009/138/ЕО на Европейския парламент и на Съвета от 25 ноември 2009 г. относно започването и упражняването на застрахователна и презастрахователна дейност (Платежоспособност II) (ОВ L 335, 17.12.2009 г., стр. 1).

⁽⁴⁹⁾ 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).

⁽⁵⁰⁾ Директива 2014/17/ЕС на Европейския парламент и на Съвета от 4 февруари 2014 г. относно договорите за кредити за жилищни недвижими имоти за потребители и за изменение на директиви 2008/48/ЕО и 2013/36/ЕС и Регламент (ЕС) № 1093/2010 (ОВ L 60, 28.2.2014 г., стр. 34).

⁽⁵¹⁾ Директива (ЕС) 2016/97 на Европейския парламент и на Съвета от 20 януари 2016 г. относно разпространението на застрахователни продукти (ОВ L 26, 2.2.2016 г., стр. 19).

Европейския парламент и на Съвета, следва да бъдат определени, в рамките на съответната им компетентност, 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 поднадзорни финансови институции, освен ако държавите членки не решат да определят друг орган, който да изпълнява тези задачи по надзор на пазара. Тези компетентни органи следва да разполагат с всички правомощия съгласно настоящия регламент и Регламент (ЕС) 2019/1020 за налагане на изпълнението на изискванията и задълженията по настоящия регламент, включително правомощия за извършване на дейности по надзор след пускане на пазара, които могат да бъдат включени, когато е целесъобразно, в техните налични надзорни механизми и процедури съгласно съответното право на Съюза в областта на финансовите услуги. Целесъобразно е да се предвиди, че когато действат като органи за надзор на пазара съгласно настоящия регламент, националните органи, отговорни за надзора над кредитните институции, регулирани съгласно Директива 2013/36/ЕС, които участват в единния надзорен механизъм, създаден с Регламент (ЕС) № 1024/2013 на Съвета⁽⁵²⁾, следва незабавно да докладват на Европейската централна банка всяка информация, установена в хода на дейностите им по надзор на пазара, която може да представлява потенциален интерес във връзка със задачите на Европейската централна банка по упражняване на пруденциален надзор, определени в посочения регламент. За да се подобри още повече съгласуваността между настоящия регламент и правилата, приложими за кредитните институции, регулирани съгласно Директива 2013/36/ЕС, е целесъобразно също така някои от процедурните задължения на доставчиците във връзка с управлението на риска, мониторинга 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 мониторинг, наложено на внедрителите на високорискови системи с ИИ, доколкото те се прилагат за кредитни институции, регулирани с Директива 2013/36/ЕС. Същият режим следва да се прилага за застрахователните и презастрахователните предприятия и застрахователните холдинги съгласно Директива 2009/138/ЕО и за застрахователните посредници съгласно Директива (ЕС) 2016/97, както и за други видове финансови институции, за които се прилагат изискванията по отношение на вътрешното управление, механизмите или процесите, установени съгласно съответното право на Съюза в областта на финансовите услуги, с цел да се гарантира последователност и равно третиране във финансовия сектор.

- (159) Всеки орган за надзор на пазара на високорисковите системи с ИИ в областта на биометричните данни, чийто списък се съдържа в приложение към настоящия регламент — доколкото системите се използват за правоохранителни цели или за целите на миграцията, убежището, управлението на граничния контрол или правораздаването и демократичните процеси — следва да разполага с ефективни правомощия за разследване и с коригиращи правомощия, включително най-малко правомощието да получава достъп до всички лични данни, които се обработват, и до цялата информация, необходима за изпълнението на неговите задачи. Органите за надзор на пазара следва да могат да упражняват правомощията си, като действат напълно независимо. Ограниченията на достъпа им до чувствителни оперативни данни съгласно настоящия регламент не следва да засягат правомощията, предоставени им с Директива (ЕС) 2016/680. Случаите, в които се изключва разкриването на данни пред националните органи за защита на данните съгласно настоящия регламент, не следва да засягат настоящите или бъдещите правомощия на тези органи извън обхвата на настоящия регламент.
- (160) Органите за надзор на пазара и Комисията следва да могат да предлагат съвместни дейности, включително съвместни разследвания, които да се провеждат от органите за надзор на пазара или от органите за надзор на пазара съвместно с Комисията, и да имат за цел насърчаване на постигането на съответствие, установяване на несъответствие, повишаване на осведомеността и осигуряване на насоки във връзка с настоящия регламент по отношение на конкретни категории високорискови системи с ИИ, за които е установено, че представляват сериозен риск в две или повече държави членки. Съвместни дейности за насърчаване на постигането на съответствие следва да се извършват съгласно член 9 от Регламент (ЕС) 2019/1020. Службата по ИИ следва да предоставя координационна подкрепа за съвместни разследвания.
- (161) Необходимо е да се изяснят отговорностите и компетентността на равнището на Съюза и на национално равнище по отношение на системите с ИИ, изградени въз основа на модели на ИИ с общо предназначение. За да се избегне припокриването на компетентност, когато дадена система с ИИ се основава на модел на ИИ с общо предназначение

⁽⁵²⁾ Регламент (ЕС) № 1024/2013 на Съвета от 15 октомври 2013 г. за възлагане на Европейската централна банка на конкретни задачи относно политиките, свързани с пруденциалния надзор над кредитните институции (ОВ L 287, 29.10.2013 г., стр. 63).

и моделът и системата се предоставят от един и същи доставчик, надзорът следва да се извършва на равнището на Съюза чрез Службата по ИИ, която следва да разполага с правомощията на орган за надзор на пазара по смисъла на Регламент (ЕС) 2019/1020 за тази цел. Във всички останали случаи националните органи за надзор на пазара продължават да носят отговорност за надзора на системите с ИИ. За системите с ИИ с общо предназначение обаче, които могат да се използват пряко от внедрителите с най-малко едно предназначение, класифицирано като високорисково, органите за надзор на пазара следва да си сътрудничат със Службата по ИИ, за да извършат оценки на съответствието, и да информират съответно Съвета по ИИ и другите органи за надзор на пазара. Освен това органите за надзор на пазара следва да могат да искат съдействие от Службата по ИИ, когато органът за надзор на пазара не е в състояние да приключи дадено разследване на високорискова система с ИИ поради невъзможност да получи достъп до определена информация, свързана с модела на ИИ с общо предназначение, въз основа на който е изградена високорисковата система с ИИ. В такива случаи следва да се прилага *mutatis mutandis* процедурата за трансгранична взаимопомощ, предвидена в глава VI от Регламент (ЕС) 2019/1020.

- (162) За да се използват по най-добрия начин централизираният експертен опит на Съюза и полезните взаимодействия на равнището на Съюза, правомощията за надзор и осигуряване на спазване по отношение на задълженията на доставчиците на модели на ИИ с общо предназначение следва да бъдат от компетентността на Комисията. Службата по ИИ следва да може да извършва всички необходими действия за мониторинг на ефективното прилагане на настоящия регламент по отношение на моделите на ИИ с общо предназначение. Тя следва да може да разследва евентуални нарушения на правилата относно доставчиците на модели на ИИ с общо предназначение както по собствена инициатива, на основание на резултатите от своите дейности по мониторинг, така и по искане на органите за надзор на пазара, в съответствие с условията, установени в настоящия регламент. За да се допринесе за извършването на ефективен мониторинг от страна на Службата по ИИ, следва да се предвиди възможността доставчиците надолу по веригата да подават жалби във връзка с евентуални нарушения на правилата относно доставчиците на модели на ИИ с общо предназначение и системи с ИИ с общо предназначение.
- (163) С цел допълване на системите за управление на моделите на ИИ с общо предназначение, експертната група следва да подпомага дейностите по мониторинг на Службата по ИИ и да може в определени случаи да отправя приоритетни сигнали до Службата по ИИ, които да водят до последващи действия, например разследвания. Такъв следва да бъде случаят, когато експертната група има основания да предполага, че даден модел на ИИ с общо предназначение представлява конкретен и установим риск на равнището на Съюза. Освен това такъв следва да бъде случаят, когато експертната група има основания да предполага, че даден модел на ИИ с общо предназначение отговаря на критериите, които биха довели до класифицирането му като модел на ИИ с общо предназначение, пораздащ системен риск. За да може експертната група да разполага с информацията, необходима за изпълнението на тези задачи, следва да има механизъм, чрез който експертната група да може да отправи искане към Комисията с цел да бъде изискана документация или информация от даден доставчик.
- (164) Службата по ИИ следва да може да предприема необходимите действия за мониторинг на ефективното изпълнение и спазване на установените в настоящия регламент задължения на доставчиците на модели на ИИ с общо предназначение. Службата за ИИ следва да може да разследва евентуални нарушения в съответствие с правомощията, предвидени в настоящия регламент, включително като изисква документация и информация, като извършва оценки, както и като изисква предприемането на мерки от доставчиците на модели на ИИ с общо предназначение. При извършването на оценките, с цел да използва независим експертен опит, Службата по ИИ следва да може да привлича независими експерти, които да извършват оценките от нейно име. Спазването на задълженията следва да бъде осигурено, наред с другото, чрез искания за предприемане на подходящи мерки, включително мерки за ограничаване на риска в случай на установени системни рискове, както и чрез ограничаване на предоставянето на пазара на даден модел, неговото изтегляне или изземване. Като гаранция в случай на необходимост, освен процесуалните права, предвидени в настоящия регламент, доставчиците на модели на ИИ с общо предназначение следва да разполагат с процесуалните права съгласно член 18 от Регламент (ЕС) 2019/1020, които следва да се прилагат, *mutatis mutandis*, без да се засягат специалните процесуални права, предвидени в настоящия регламент.
- (165) 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 етичен и надежден ИИ в Съюза. Доставчиците на системи с ИИ, които не са високорискови, следва да бъдат насърчавани да изготвят кодекси за поведение, включително свързани с тях управленски механизми, предназначени да поощряват прилагането на доброволна основа на някои или на всички задължителни изисквания, приложими за високорисковите системи с ИИ и адаптирани с оглед на предназначението на системите и по-ниския риск, като вземат предвид наличните технически решения и най-добрите практики в сектора, например карти за модели и данни. Доставчиците и, когато е целесъобразно, внедрителите на всички системи с ИИ — високорискови или не, както и на всички модели с ИИ, следва също да бъдат насърчавани да прилагат на доброволна основа допълнителни изисквания, свързани например с елементи на Насоките на Съюза относно етичните аспекти за надежден ИИ, екологичната устойчивост, мерките относно грамотността

в областта на ИИ, приобщаващия характер и многообразието при проектирането и разработването на системи с ИИ, включително повишеното внимание към уязвимите лица и достъпността за хора с увреждания, участието на заинтересованите страни чрез привличане, когато е целесъобразно, на заинтересовани страни като професионални организации и организации на гражданското общество, академични среди, научноизследователски организации, синдикати и организации за защита на потребителите, в проектирането и разработването на системи с ИИ, както и многообразието на екипите от разработчици, включително баланса между половете. За да се гарантира, че незадължителните кодекси за поведение са ефективни, те следва да се основават на ясни цели и ключови показатели за ефективност, за да може да бъде оценено постигането на тези цели. Те следва също така да бъдат разработени по приобщаващ начин, когато е целесъобразно – с участието на съответните заинтересовани страни, като професионални организации и организации на гражданското общество, академични среди, научноизследователски организации, синдикати и организации за защита на потребителите. Комисията може да разработва инициативи, включително от секторен характер, за да улесни преодоляването на техническите пречки пред трансграничния обмен на данни за разработването на ИИ, включително свързаните с инфраструктурата за достъп до данни и семантичната и техническата оперативна съвместимост на различните видове данни.

- (166) 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, установени за високорисковите системи с ИИ, да бъдат въпреки това безопасни при пускането им на пазара или пускането им в действие. За да се допринесе за постигането на тази цел, допълнителна гаранция ще представлява възможността за прилагане на Регламент (ЕС) 2023/988 на Европейския парламент и на Съвета⁽⁵³⁾.
- (167) 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, в съответствие с правото на Съюза и националното право. Те следва да изпълняват задачите и дейностите си по такъв начин, че да закрилят по-специално правата върху интелектуалната собственост, поверителната търговска информация и търговските тайни, ефективното прилагане на настоящия регламент, обществените интереси и националната сигурност, независимостта на наказателните или административните производства и неприкосновеността на класифицираната информация.
- (168) Спазването на настоящия регламент следва да може да се гарантира чрез налагането на санкции и други мерки за изпълнение. 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 да осигурят зачитането на принципа *non bis in idem*. С цел подсилване и хармонизиране на административните санкции за нарушения на настоящия регламент, следва да се установят горните граници за определяне на административните глоби и имуществени санкции за някои конкретни нарушения. При определянето на размера на глобите и имуществените санкции държавите членки следва във всеки отделен случай да вземат предвид всички обстоятелства на конкретния случай, като надлежно отчитат по-специално естеството, тежестта и продължителността на нарушението и неговите последици, както и размера на доставчика, по-специално ако доставчикът е МСП, включително новосъздадено предприятие. Европейският надзорен орган по защита на данните следва да има правомощията да налага глоби на институциите, агенциите и органите на Съюза, попадащи в обхвата на настоящия регламент.
- (169) Спазването на задълженията на доставчиците на модели на ИИ с общо предназначение, наложени с настоящия регламент, следва да може да се гарантира, наред с другото, чрез глоби. За тази цел следва да се определят и подходящи размери на глобите за нарушение на тези задължения, включително неизпълнението на мерките, изисквани от Комисията в съответствие с настоящия регламент, при прилагане на подходящи давностни срокове в съответствие с принципа на пропорционалност. Всички решения, приемани от Комисията съгласно настоящия регламент, подлежат на контрол от Съда на Европейския съюз в съответствие с ДФЕС, включително на пълната юрисдикция на Съда във връзка със санкциите съгласно член 261 ДФЕС.
- (170) В правото на Съюза и националното право вече са предвидени ефективни правни средства за защита на физическите и юридическите лица, чиито права и свободи са неблагоприятно засегнати от използването на системи с ИИ. Без да се засягат тези правни средства за защита, всяко физическо или юридическо лице, което има основания да счита, че е налице нарушение на настоящия регламент, следва да има правото да подаде жалба до съответния орган за надзор на пазара.
- (171) Засегнатите лица следва да имат правото да получат обяснение, в случай че дадено решение, взето от внедрител преди всичко въз основа на резултата от работата на определени високорискови системи с ИИ, попадащи в обхвата на настоящия регламент, поражда правни последици за тях или по сходен начин ги засяга в значителна степен по начин,

⁽⁵³⁾ Регламент (ЕС) 2023/988 на Европейския парламент и на Съвета от 10 май 2023 г. относно общата безопасност на продуктите, за изменение на Регламент (ЕС) № 1025/2012 на Европейския парламент и на Съвета и на Директива (ЕС) 2020/1828 на Европейския парламент и на Съвета и за отмяна на Директива 2001/95/ЕО на Европейския парламент и на Съвета и на Директива 87/357/ЕО на Съвета (ОВ L 135, 23.5.2023 г., стр. 1).

който според тях оказва неблагоприятно въздействие върху тяхното здраве, безопасност или основни права. Това обяснение следва да бъде ясно и изчерпателно и да дава основание на засегнатите лица да упражнят правата си. Правото на получаване на обяснение не следва да се прилага относно използването на системи с ИИ, по отношение на които от правото на Съюза или от националното право произтичат изключения или ограничения, и следва да се прилага само доколкото това право все още не е предвидено в законодателството на Съюза.

- (172) Лица, сигнализиращи за нередности във връзка с нарушения на настоящия регламент, следва да бъдат защитени в съответствие с правото на Съюза. Поради това по отношение на подаването на сигнали за нарушения на настоящия регламент и защитата на лицата, които подават сигнали за такива нарушения, следва да се прилага Директива (ЕС) 2019/1937 на Европейския парламент и на Съвета⁽⁵⁴⁾.
- (173) С цел да се гарантира, че регулаторната рамка може да бъде адаптирана при необходимост, на Комисията следва да бъде делегирано правомощието да приема актове в съответствие с член 290 ДФЕС за изменение на условията, при които дадена система с ИИ не се смята за високорискова, списъка на високорисковите системи с ИИ, разпоредбите относно техническата документация, съдържанието на ЕС декларацията за съответствие, разпоредбите относно процедурите за оценяване на съответствието, разпоредбите за определяне 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, праговете, референтните стойности и показателите, включително чрез допълване на тези референтни стойности и показатели, в правилата за класифициране на моделите на ИИ с общо предназначение, пораждащи системен риск, техническата документация за доставчиците на модели на ИИ с общо предназначение и информацията с цел прозрачност за доставчиците на модели на ИИ с общо предназначение. 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, заложи в Междуйнституционалното споразумение от 13 април 2016 г. за по-добро законотворчество⁽⁵⁵⁾. По-специално, с цел осигуряване на равно участие при подготовката на делегираните актове, Европейският парламент и Съветът получават всички документи едновременно с експертите от държавите членки, като техните експерти получават систематично достъп до заседанията на експертните групи на Комисията, занимаващи се с подготовката на делегираните актове.
- (174) Предвид бързото технологично развитие и техническия експертен опит, необходим за ефективното прилагане на настоящия регламент, Комисията следва да направи оценка и преглед на настоящия регламент до 2 август 2029 г. и на всеки четири години след това, и да докладва на Европейския парламент и на Съвета. Освен това, с оглед на последиците за обхвата на настоящия регламент, Комисията следва веднъж годишно да прави оценка на необходимостта от изменение на списъка на високорисковите системи с ИИ и на списъка на забранените практики. Наред с това, до 2 август 2028 г. и на всеки четири години след това Комисията следва да оценява и да докладва на Европейския парламент и на Съвета за необходимостта от изменение на наименованията на високорисковите области в приложението към настоящия регламент, системите с ИИ, попадащи в обхвата на задълженията за прозрачност, ефективността на системата за надзор и управление и напредъка по разработването на стандартизационни документи за енергийно ефективно разработване на модели на ИИ с общо предназначение, включително за необходимостта от допълнителни мерки или действия. И на последно място, до 2 август 2028 г. и на всеки три години след това Комисията следва да оценява въздействието и ефективността на незадължителните кодекси за поведение с цел да се насърчи прилагането на изискванията, предвидени за високорисковите системи с ИИ, по отношение на системи, различни от високорискови системи с ИИ, и евентуално на други допълнителни изисквания за такива системи с ИИ.
- (175) 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 Съвета⁽⁵⁶⁾.
- (176) Доколкото целта на настоящия регламент, а именно да се подобри функционирането на вътрешния пазар и да се насърчи навлизането на ориентиран към човека и надежден ИИ, като същевременно се гарантира високо равнище на защита на здравето, безопасността, основните права, залегнали в Хартата, включително демокрацията, принципите на правовата държава и опазването на околната среда, срещу вредното въздействие на системите с ИИ в Съюза и да се подкрепят иновациите, 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

⁽⁵⁴⁾ Директива (ЕС) 2019/1937 на Европейския парламент и на Съвета от 23 октомври 2019 г. относно защитата на лицата, които подават сигнали за нарушения на правото на Съюза (ОВ L 305, 26.11.2019 г., стр. 17).

⁽⁵⁵⁾ ОВ L 123, 12.5.2016 г., стр. 1.

⁽⁵⁶⁾ 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).

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.

- (177) С цел да се гарантира правна сигурност, да се осигури подходящ срок за адаптация за операторите и да се избегнат смущения на пазара, включително чрез осигуряване на непрекъснатост в използването на системите с ИИ, е целесъобразно настоящият регламент да се прилага за високорисковите системи с ИИ, които са били пуснати на пазара или пуснати в действие преди общата начална дата на прилагането му, само в случай че след тази дата бъдат извършени значителни промени в проекта или предназначението на тези системи. Следва да се поясни, че в този контекст понятието „значителна промяна“ следва да се разбира като равностойно по същество на понятието „съществено изменение“, което се използва само по отношение на високорисковите системи с ИИ съгласно определението в настоящия регламент. По изключение и с оглед на публичната отчетност операторите на системи с ИИ, които са компоненти на широкомащабните информационни системи, създадени с правните актове, чийто списък е приложен към настоящия регламент, и операторите на високорискови системи с ИИ, предназначени да бъдат използвани от публични органи, следва да предприемат мерките, необходими, за да се съобразят с изискванията на настоящия регламент, съответно до края на 2030 г. и в срок до 2 август 2030 г.
- (178) Доставчиците на високорискови системи с ИИ се насърчават да започнат да спазват на доброволна основа съответните задължения, предвидени съгласно настоящия регламент, още по време на преходния период.
- (179) Настоящият регламент следва да се прилага от 2 август 2026 г. Същевременно, като се има предвид неприемливият риск, свързан с използването на ИИ по определени начини, забраните, както и общите разпоредби на настоящия регламент следва да се прилагат още от 2 февруари 2025 г. Въпреки че тези забрани ще влязат напълно в действие, след като бъде установено управлението и прилагането на настоящия регламент, предварителното им прилагане е важно с оглед да се вземе предвид неприемливият риск и да се въздейства върху други процедури, например в гражданското право. Наред с това, инфраструктурата, свързана с управлението и системата за оценяване на съответствието, следва да започне да функционира преди 2 август 2026 г., поради което разпоредбите относно нотифицираните органи и структурата на управление следва да се прилагат от 2 август 2025 г. Като се има предвид бързият темп на технологичния напредък и възприемането на модели на ИИ с общо предназначение, задълженията на доставчиците на модели на ИИ с общо предназначение следва да се прилагат от 2 август 2025 г. Кодексите за добри практики следва да бъдат готови в срок до 2 май 2025 г., за да се даде възможност на доставчиците своевременно да докажат спазването им. Службата по ИИ следва да гарантира, че правилата и процедурите за класифициране са актуални с оглед на технологичното развитие. Освен това държавите членки следва да установят и изпратят до Комисията правилата относно санкциите, включително административните глоби и имуществени санкции, и да гарантират, че те се прилагат правилно и ефективно към началната дата на прилагане на настоящия регламент. Поради това разпоредбите относно санкциите следва да се прилагат от 2 август 2025 г.
- (180) В съответствие с член 42, параграфи 1 и 2 от Регламент (ЕС) 2018/1725 беше проведена консултация с Европейския надзорен орган по защита на данните и Европейския комитет по защита на данните, които представиха съвместното си становище на 18 юни 2021 г.,

ПРИЕХА НАСТОЯЩИЯ РЕГЛАМЕНТ:

ГЛАВА I

ОБЩИ РАЗПОРЕДБИ

Член 1

Предмет

1. Целта на настоящия регламент е да се подобри функционирането на вътрешния пазар и да се насърчи навлизането на ориентиран към човека и надежден изкуствен интелект (ИИ), като същевременно се осигурява високо равнище на защита на здравето, безопасността, основните права, залегнали в Хартата, включително демокрацията, принципите на правовата държава и опазването на околната среда, от вредните въздействия на системите с ИИ в Съюза, както и да се подкрепят иновациите.

2. С настоящия регламент се установяват:

а) хармонизирани правила за пускането на пазара, пускането в действие и използването на системи с ИИ в Съюза;

- б) забрани на определени практики в областта на ИИ;
- в) особени изисквания за високорисковите системи с ИИ и задължения за операторите на такива системи;
- г) хармонизирани правила за прозрачност за определени системи с ИИ;
- д) хармонизирани правила за пускането на пазара на модели на ИИ с общо предназначение;
- е) правила за мониторинг на пазара, надзор на пазара, управление и осигуряване на спазването;
- ж) мерки в подкрепа на иновациите с особено внимание към МСП, включително новосъздадените предприятия.

Член 2

Обхват

1. Настоящият регламент се прилага по отношение на:

- а) доставчици, които пускат на пазара или пускат в действие системи с ИИ или пускат на пазара модели на ИИ с общо предназначение в Съюза, независимо дали тези доставчици са установени или се намират на територията на Съюза или в трета държава;
- б) внедрители на системи с ИИ, чието място на установяване е на територията на Съюза или които се намират на територията на Съюза;
- в) доставчици и внедрители на системи с ИИ, чието място на установяване е в трета държава или които се намират в трета държава, когато резултатът, получен от системата с ИИ, се използва в Съюза;
- г) вносители и дистрибутори на системи с ИИ;
- д) производители на продукти, които пускат на пазара или пускат в действие система с ИИ заедно със своя продукт и със своето име или търговска марка;
- е) упълномощени представители на доставчици, които не са установени в Съюза;
- ж) засегнати лица, които се намират в Съюза.

2. За системи с ИИ, които са класифицирани като високорискови системи с ИИ в съответствие с член 6, параграф 1, които са свързани с продукти, обхванати от законодателството на Съюза за хармонизация, посочено в раздел Б от приложение I, се прилагат само член 6, параграф 1 и членове 102 – 109 и 112. Член 57 се прилага само доколкото изискванията за високорисковите системи с ИИ съгласно настоящия регламент са били включени в това законодателство на Съюза за хармонизация.

3. Настоящият регламент не се прилага в области извън обхвата на правото на Съюза и не засяга компетентността на държавите членки по отношение на националната сигурност, независимо от вида на субекта, на който държавите членки са възложили изпълнението на задачите във връзка с тази компетентност.

Настоящият регламент не се прилага за системи с ИИ, ако и доколкото те са пуснати на пазара, пуснати в действие или използвани със или без изменение на тези системи изключително за военни цели и цели, свързани с отбраната или националната сигурност, независимо от вида на субекта, който извършва тези дейности.

Настоящият регламент не се прилага за системи с ИИ, които не са пуснати на пазара или пуснати в действие в Съюза, когато резултатите се използват в Съюза изключително за военни цели и цели, свързани с отбраната или националната сигурност, независимо от вида на субекта, който извършва тези дейности.

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 международно сътрудничество или споразумения за правоприлагане и съдебно сътрудничество със Съюза или с една или повече държави членки, при условие че тази трета държава или международна организация осигурява подходящи гаранции по отношение на защитата на основните права и свободи на физическите лица.

5. Настоящият регламент не засяга прилагането на разпоредбите относно отговорността на доставчиците на посреднически услуги, установени в глава II от Регламент (ЕС) 2022/2065.

6. Настоящият регламент не се прилага за системите с ИИ или моделите на ИИ, които са специално разработени и пуснати в действие единствено с цел научноизследователска и развойна дейност, включително за техните резултати.
7. Правото на Съюза относно защитата на личните данни, неприкосновеността на личния живот и поверителността на съобщенията се прилага за личните данни, обработвани във връзка с правата и задълженията, предвидени в настоящия регламент. Настоящият регламент не засяга регламенти (ЕС) 2016/679 и (ЕС) 2018/1725, нито директиви 2002/58/ЕО и (ЕС) 2016/680, без да се засягат член 10, параграф 5 и член 59 от настоящия регламент.
8. Настоящият регламент не се прилага за научноизследователски дейности, изпитвания или развойни дейности по отношение на системи с ИИ или модели на ИИ преди пускането на пазара или пускането в действие на тези системи или модели. Тези дейности се извършват в съответствие с приложимото право на Съюза. Изпитването в реални условия не попада в обхвата на това изключение.
9. Настоящият регламент не засяга правилата, установени в други правни актове на Съюза, свързани със защитата на потребителите и безопасността на продуктите.
10. Настоящият регламент не се прилага за задълженията на внедрители, които са физически лица, използващи системи с ИИ в рамките на изцяло лична непрофесионална дейност.
11. Настоящият регламент не е пречка Съюзът или държавите членки да запазят или въведат закони, подзаконови или административни разпоредби, които са по-благоприятни за работниците по отношение на защитата на правата им във връзка с използването от работодателите на системи с ИИ, нито да насърчават или разрешават прилагането на колективни трудови договори, които са по-благоприятни за работниците.
12. Настоящият регламент не се прилага за системи с ИИ, предоставени с безплатен лиценз с отворен код, освен ако не са пуснати на пазара или пуснати в действие като високорискови системи с ИИ или като система с ИИ, попадаща в обхвата на член 5 или 50.

Член 3

Определения

За целите на настоящия регламент се прилагат следните определения:

- 1) „система с ИИ“ означава машинно базирана система, която е проектирана да работи с различни нива на автономност и която може да прояви адаптивност след внедряването си, и която, с явна или подразбираща се цел, въз основа на въведените в нея входящи данни, извежда начина на генериране на резултати като прогнози, съдържание, препоръки или решения, които могат да окажат влияние върху физическа или виртуална среда;
- 2) „риск“ означава съчетанието от вероятността за възникване на дадена вреда и тежестта на тази вреда;
- 3) „доставчик“ означава физическо или юридическо лице, публичен орган, агенция или друга организация, които разработват система с ИИ или модел на ИИ с общо предназначение или възлагат разработването на система с ИИ или на модел на ИИ с общо предназначение и ги пускат на пазара, или пускат в действие системата с ИИ със своето име или търговска марка, срещу заплащане или безплатно;
- 4) „внедрител“ означава физическо или юридическо лице, публичен орган, агенция или друга организация, които използват система с ИИ, по отношение на която упражняват контрол, с изключение на случаите, когато системата с ИИ се използва в процеса на лична непрофесионална дейност;
- 5) „упълномощен представител“ означава физическо или юридическо лице, намиращо се или установено в Съюза, което е получило и приело писмено пълномощно от доставчик на система с ИИ или на модел на ИИ с общо предназначение съответно да изпълнява и извършва от негово име задълженията и процедурите, установени в настоящия регламент;
- 6) „вносител“ означава физическо или юридическо лице, намиращо се или установено в Съюза, което пуска на пазара система с ИИ, носеща името или търговската марка на физическо или юридическо лице, установено в трета държава;
- 7) „дистрибутор“ означава физическо или юридическо лице във веригата на доставки, различно от доставчика или вносителя, което предоставя система с ИИ на пазара на Съюза;
- 8) „оператор“ означава доставчик, производител на продукти, внедрител, упълномощен представител, вносител или дистрибутор;

- 9) „пускане на пазара“ означава предоставянето на система с ИИ или на модел на ИИ с общо предназначение на пазара на Съюза за първи път;
- 10) „предоставяне на пазара“ означава всяка доставка на система с ИИ или на модел на ИИ с общо предназначение за дистрибуция или използване на пазара на Съюза в процеса на търговска дейност, срещу заплащане или безплатно;
- 11) „пускане в действие“ означава доставката на система с ИИ за първо използване пряко на внедрителя или за собствено ползване в Съюза в съответствие с нейното предназначение;
- 12) „предназначение“ означава използването, за което е предназначена една система с ИИ от доставчика, включително конкретният контекст и условия на използване, 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“ означава използването на система с ИИ по начин, който не е в съответствие с нейното предназначение, но е възможно да бъде резултат от разумно предвидимо човешко поведение или от взаимодействие с други системи, включително други системи с ИИ;
- 14) „защитен елемент“ означава компонент на продукт или система с ИИ, който осигурява функция, свързана с безопасността, за този продукт или тази система с ИИ или чиято неизправност или лошо функциониране поставя в опасност здравето и безопасността на хора или имущество;
- 15) „инструкции за употреба“ означава информацията, която доставчикът предоставя с цел да информира внедрителя по-специално за предназначението и правилното използване на дадена система с ИИ;
- 16) „изземване на система с ИИ“ означава всяка мярка, целяща да постигне връщане на доставчика, извеждане от действие или блокиране на използването на система с ИИ, която е предоставена на внедрителите;
- 17) „изтегляне на система с ИИ“ означава всяка мярка, целяща да предотврати предоставянето на пазара на система с ИИ, която е във веригата на доставки;
- 18) „действие на система с ИИ“ означава способността на дадена система с ИИ да изпълнява предназначението си;
- 19) „нотифициращ орган“ означава националният орган, отговорен за въвеждането и извършването на процедурите, необходими за оценката, 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 доказване дали са изпълнени изискванията, установени в глава III, раздел 2 по отношение на дадена високорискова система с ИИ;
- 21) „орган за оценяване на съответствието“ означава орган, който осъществява дейности по оценяване на съответствието от трето лице, включително изпитване, сертификация и контрол;
- 22) „нотифициран орган“ означава орган за оценяване на съответствието, нотифициран съгласно настоящия регламент и друго приложимо законодателство на Съюза за хармонизация;
- 23) „съществено изменение“ означава промяна в дадена система с ИИ след пускането ѝ на пазара или пускането ѝ в действие, която не е предвидена или планирана в първоначалното оценяване на съответствието от доставчика и в резултат на която се засяга съответствието на системата с ИИ с изискванията, установени в глава III, раздел 2, или която води до изменение на предназначението, за което е била оценена системата с ИИ;
- 24) „маркировка „СЕ““ означава маркировка, чрез която доставчикът указва, че дадена система с ИИ е в съответствие с изискванията, установени в глава III, раздел 2 от настоящия регламент и в друго приложимо законодателство на Съюза за хармонизация, предвиждащо нанасянето на тази маркировка;
- 25) „система за мониторинг след пускането на пазара“ означава всички дейности, извършвани от доставчиците на системи с ИИ с цел събиране и преглед на опита, натрупан при използването на системите с ИИ, които са пуснали на пазара или пуснали в действие, с оглед на установяване на евентуална необходимост от незабавно прилагане на всякакви необходими коригиращи или превантивни действия;
- 26) „орган за надзор на пазара“ означава националният орган, който извършва дейностите и предприема мерките съгласно Регламент (ЕС) 2019/1020;

- 27) „хармонизиран стандарт“ означава хармонизиран стандарт съгласно определението в член 2, параграф 1, буква в) от Регламент (ЕС) № 1025/2012;
- 28) „обща спецификация“ означава набор от технически спецификации съгласно определението в член 2, точка 4 от Регламент (ЕС) № 1025/2012, даващи възможност да се постигне съответствие с определени изисквания, установени съгласно настоящия регламент;
- 29) „обучителни данни“ означава данни, използвани за обучение на система с ИИ чрез настройка на нейните обучавани параметри;
- 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 недостатъчно или прекомерно настройване;
- 31) „набор от валидационни данни“ означава отделен набор от данни или част от набора обучителни данни под формата на фиксирано или променливо разделяне на данните;
- 32) „изпитвателни данни“ означава данни, използвани за извършване на независима оценка на системата с ИИ с цел потвърждаване на очакваното действие на тази система преди пускането ѝ на пазара или пускането ѝ в действие;
- 33) „входящи данни“ означава данни, предоставяни на система с ИИ или пряко придобивани от нея, въз основа на които системата произвежда резултат;
- 34) „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, например лицеви изображения или дактилоскопични данни;
- 35) „биометрична идентификация“ означава автоматизирано разпознаване на физически, физиологични, поведенчески и психологически човешки характеристики с цел установяване на самоличността на дадено физическо лице чрез съпоставяне на биометрични данни на това лице с биометрични данни на лица, съхранявани в база данни;
- 36) „биометрична проверка“ означава автоматизирана проверка „едно към едно“, включително удостоверяване, на самоличността на физически лица чрез съпоставяне на техните биометрични данни с предварително предоставени биометрични данни;
- 37) „специални категории лични данни“ означава категориите 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;
- 38) „чувствителни оперативни данни“ означава оперативни данни, свързани с дейности по предотвратяване, откриване, разследване и наказателно преследване на престъпления, разкриването на които може да застраши независимостта на наказателните производства;
- 39) „система за разпознаване на емоции“ означава система с ИИ, чието предназначение е да определя или да прави заключения за емоциите или намеренията на физически лица на базата на техните биометрични данни;
- 40) „система за биометрично категоризиране“ означава система с ИИ, предназначена да отнася физически лица към конкретни категории въз основа на техните биометрични данни, освен когато тази система е чисто спомагателна по отношение на друга търговска услуга и е строго необходима по обективни технически причини;
- 41) „система за дистанционна биометрична идентификация“ означава система с ИИ, предназначена да идентифицира физически лица обикновено от разстояние, без тяхното активно участие, чрез съпоставяне на биометричните данни на дадено лице с биометричните данни, съдържащи се в референтно хранилище на данни;
- 42) „система за дистанционна биометрична идентификация в реално време“ означава система за дистанционна биометрична идентификация, при която снемането на биометрични данни, съпоставянето и идентификацията се осъществяват без значително забавяне, включваща не само незабавното идентифициране, но и ограничени кратки забавяния с цел предотвратяване на заобикаляне на системата;
- 43) „система за последваща дистанционна биометрична идентификация“ означава система за дистанционна биометрична идентификация, различна от система за дистанционна биометрична идентификация в реално време;
- 44) „обществено достъпно място“ означава всяко физическо място, което е публична или частна собственост и е достъпно за неопределен брой физически лица, независимо от прилагането на определени условия за достъп и независимо от евентуални ограничения на капацитета;

- 45) „правоохранителен орган“ означава:
- а) всеки публичен орган, който има правомощия за предотвратяване, разследване, откриване или наказателно преследване на престъпления или за изпълнение на наказателноправни санкции, включително за предпазване от заплахи за обществената сигурност и тяхното предотвратяване; или
 - б) всяка друга организация или субект, на която или на който съгласно правото на държава членка е възложено да упражнява публична власт и публични правомощия за целите на предотвратяването, разследването, откриването или наказателното преследване на престъпления или изпълнението на наказателноправни санкции, включително предпазването от заплахи за обществената сигурност и тяхното предотвратяване;
- 46) „правоохранителна дейност“ означава действия, извършвани от правоохранителните органи или от тяхно име за предотвратяване, разследване, откриване или наказателно преследване на престъпления или за изпълнение на наказателноправни санкции, включително за предпазване от заплахи за обществената сигурност и тяхното предотвратяване;
- 47) „Служба по ИИ“ означава функцията на Комисията да допринася за прилагането, мониторинга и надзора на системите с ИИ и моделите на ИИ с общо предназначение и управлението на ИИ, предвидена в Решение на Комисията от 24 януари 2024 г.; позоваванията на Службата по ИИ в настоящия регламент се разбират като позовавания на Комисията;
- 48) „национален компетентен орган“ означава нотифициращ орган или орган за надзор на пазара; по отношение на системите с ИИ, пуснати в действие или използвани от институциите, агенциите, службите и органите на Съюза, всяко позоваване на националните компетентни органи или органите за надзор на пазара в настоящия регламент се тълкува като позоваване на Европейския надзорен орган по защита на данните;
- 49) „сериозен инцидент“ означава всеки инцидент или неизправност на система с ИИ, който или която пряко или косвено води до някоя от следните последици:
- а) смъртта на човек или сериозно увреждане на здравето на човек;
 - б) сериозно и необратимо нарушаване на управлението и експлоатацията на критична инфраструктура;
 - в) нарушение на задължения съгласно правото на Съюза, имащи за цел да защитава основните права;
 - г) сериозно увреждане на имущество или на околната среда;
- 50) „лични данни“ означава лични данни съгласно определението в член 4, точка 1 от Регламент (ЕС) 2016/679;
- 51) „нелични данни“ означава данни, различни от личните данни съгласно определението в член 4, точка 1 от Регламент (ЕС) 2016/679;
- 52) „профилиране“ означава профилиране съгласно определението в член 4, точка 4 от Регламент (ЕС) 2016/679;
- 53) „план за изпитване в реални условия“ означава документ, в който се описват целите, методиката, териториалният, демографският и времевият обхват, мониторингът, организацията и провеждането на изпитвания в реални условия;
- 54) „план за лабораторията“ означава документ, договорен между участващия доставчик и компетентния орган, в който се описват целите, условията, графикът, методиката и изискванията по отношение на дейностите, извършвани в рамките на лабораторията;
- 55) „регулаторна лаборатория в областта на ИИ“ означава контролирана рамка, създадена от компетентен орган, която осигурява на доставчиците или потенциалните доставчици на системи с ИИ възможност да разработват, обучават, валидират и изпитват, когато е целесъобразно в реални условия, иновативна система с ИИ, съгласно плана за лабораторията и в рамките на ограничен срок под регулаторен надзор;
- 56) „грамотност в областта на ИИ“ означава уменията, знанията и разбирането, благодарение на които доставчиците, внедрителите и засегнатите лица — като се отчитат съответните им права и задължения в контекста на настоящия регламент — могат да внедряват системи с ИИ по информиран начин, както и да се осведомяват за възможностите и рисковете, свързани с ИИ, и за евентуалните вреди, които той може да причини;

- 57) „изпитване в реални условия“ означава временното изпитване на система с ИИ в съответствие с нейното предназначение в реални условия извън лаборатория или симулирана по друг начин среда с цел събиране на надеждни и солидни данни и оценяване и проверка на съответствието на системата с ИИ с изискванията на настоящия регламент, като това не се счита за пускане на системата с ИИ на пазара или за пускането ѝ в действие по смисъла на настоящия регламент, при условие че са изпълнени всички условия, посочени в член 57 или 60;
- 58) „субект в изпитване“ за целите на изпитването в реални условия означава физическо лице, което участва в изпитване в реални условия;
- 59) „информирано съгласие“ означава свободно, конкретно, недвусмислено и доброволно изразяване от страна на даден субект в изпитване на готовността му да участва в определено изпитване в реални условия, след като е бил информиран за всички аспекти на изпитването, които са от значение за решението за участие на субекта в изпитването;
- 60) „убедителен фалшификат“ означава генерирано или обработено изображение, аудио- или видео съдържание, което наподобява съществуващи лица, предмети, места, субекти или събития и създава погрешно впечатление у дадено лице, че е автентично или достоверно;
- 61) „широко разпространено нарушение“ означава всяко действие или бездействие, което е в разрез с правото на Съюза за защита на интересите на физическите лица и което:
- a) е увредило или има вероятност да увреди колективните интереси на физически лица, пребиваващи в най-малко две държави членки, различни от държавата членка, в която:
 - i) е започнало или е извършено действието или бездействието;
 - ii) е установен или се намира съответният доставчик или, когато е приложимо, неговият упълномощен представител; или
 - iii) е установен внедрителят, когато нарушението е извършено от внедрителя;
 - b) е увредило, уврежда или има вероятност да увреди колективните интереси на физически лица, има общи характеристики, включително едни и същи незаконни практики или нарушаване на едни и същи интереси, и се проявява едновременно, като се извършва от един и същи оператор в най-малко три държави членки;
- 62) „критична инфраструктура“ означава критична инфраструктура съгласно определението в член 2, точка 4 от Директива (ЕС) 2022/2557;
- 63) „модел на ИИ с общо предназначение“ означава модел на ИИ, включително когато такъв модел е обучен с голямо количество данни, като се използва самонадзор в голям мащаб, който има до голяма степен общ характер и е в състояние компетентно да изпълнява широк набор от отделни задачи, независимо от начина на пускане на модела на пазара, и който може да бъде интегриран в различни системи или приложения надолу по веригата, с изключение на моделите на ИИ, използвани за научноизследователски и развойни дейности и като прототипи преди пускането им на пазара;
- 64) „способности с висока степен на въздействие“ означава способности, които съответстват на или надхвърлят способностите, регистрирани в най-напредналите модели на ИИ с общо предназначение;
- 65) „системен риск“ означава риск, присъщ за способностите с висока степен на въздействие на моделите на ИИ с общо предназначение, които оказват значително въздействие върху пазара на Съюза поради своя обхват или поради реалните си или разумно предвидими отрицателни последици върху общественото здраве, безопасността, обществената сигурност, основните права или обществото като цяло, който може да се разпространи в голям мащаб по цялата верига за създаване на стойност;
- 66) „система с ИИ с общо предназначение“ означава система с ИИ, основана на модел на ИИ с общо предназначение, която може да служи за различни цели и може да се използва пряко, както и да се интегрира в други системи с ИИ;
- 67) „операция с плаваща запетая“ означава всяка математическа операция или присвояване, включващи числа с плаваща запетая, които са подмножество на реалните числа и при компютрите обикновено се представят чрез цяло число с фиксирана точност, мащабирано с цял експонент с фиксирана основа;
- 68) „доставчик надолу по веригата“ означава доставчик на система с ИИ, включително на система с ИИ с общо предназначение, която включва модел на ИИ, независимо дали моделът на ИИ се предоставя от самия него и е вертикално интегриран, или се предоставя от друг субект въз основа на договорни отношения.

Член 4

Грамотност в областта на ИИ

Доставчиците и внедрителите на системи с ИИ предприемат всички възможни мерки, за да гарантират достатъчно ниво на грамотност в областта на ИИ на техния персонал и другите лица, занимаващи се с функционирането и използването на системите с ИИ от тяхно име, като отчитат техните технически познания, опит, образование и обучение, както и контекста, в който ще се използват системите с ИИ, и вземат предвид лицата или групите лица, по отношение на които ще се използват системите с ИИ.

ГЛАВА II

ЗАБРАНЕНИ ПРАКТИКИ

Член 5

Забранени практики в областта на ИИ

1. Забраняват се следните практики в областта на ИИ:
 - а) пускането на пазара, пускането в действие или използването на система с ИИ, която си служи със техники, действащи на подсъзнанието и отвъд рамките на съзнаването от човека, или с умишлено манипулативни или измамни техники, с цел или последици, изразяващи се в съществено изменение на поведението на дадено лице или група лица чрез значително нарушаване на способността за вземане на информирано решение, като по този начин се подтиква да вземе решение, което в противен случай не би взело, по начин, който причинява или има разумна вероятност да причини значителни вреди на същото или на друго лице, или на група лица;
 - б) пускането на пазара, пускането в действие или използването на система с ИИ, която използва някое от уязвимите места на дадено физическо лице или на конкретна група лица, дължащи се на възраст, увреждане или конкретно социално или икономическо положение, с цел или последици, изразяващи се в съществено изменение на поведението на това лице или на лице, спадащо към тази група, по начин, който причинява или има разумна вероятност да причини значителни вреди на същото или на друго лице;
 - в) пускането на пазара, пускането в действие или използването на системи с ИИ с цел оценка или класифициране на физически лица или групи от лица през определен период от време въз основа на тяхното социално поведение или известни, изведени или предполагаеми лични или личностни характеристики, като социалната класация води до едната или и до двете посочени по-долу последици:
 - i) увреждащо или неблагоприятно третиране на определени физически лица или на групи лица в социален контекст, който няма връзка с контекста, в който първоначално са били генерирани или събрани данните;
 - ii) увреждащо или неблагоприятно третиране на определени физически лица или на групи лица, което е неоправдано или непропорционално с оглед на тяхното социално поведение или на тежестта, която му се отдава;
 - г) пускането на пазара, пускането в действие с това конкретно предназначение или използването на система с ИИ за извършване на оценки на риска по отношение на физически лица с цел да се прецени или предвиди вероятността дадено физическо лице да извърши престъпление, въз основа единствено на профилирането на дадено физическо лице или на оценката на личностните му черти и характеристики; тази забрана не се прилага за системи с ИИ, използвани за подпомагане на извършването от човек на оценка на участието на дадено лице в престъпна дейност, която вече е изградена на основата на обективни и проверими факти, пряко свързани с престъпна дейност;
 - д) пускането на пазара, пускането в действие с това конкретно предназначение или използването на системи с ИИ, които създават или разширяват бази данни за разпознаване на лица чрез нецеленасочено извличане на лицеве изображения от интернет или записи от видеонаблюдение;
 - е) пускането на пазара, пускането в действие с това конкретно предназначение или използването на системи с ИИ с цел да се направят заключения за емоциите на дадено физическо лице на работното място или в образователните институции, освен в случаите, когато системата с ИИ е предназначена да бъде внедрена или пусната на пазара по медицински съображения или съображения, свързани с безопасността;

- ж) пускането на пазара, пускането в действие с това конкретно предназначение или използването на системи за биометрично категоризиране, които категоризират по индивидуализиран начин физическите лица въз основа на техните биометрични данни с цел да се направят заключения или логически изводи за тяхната раса, политически възгледи, членство в синдикални организации, религиозни или философски убеждения, сексуален живот или сексуална ориентация; тази забрана не обхваща обозначаването или филтрирането на законно придобити набори от биометрични данни, например основани на биометрични данни изображения, или категоризиране на биометрични данни в правоохранителната област;
- з) използването на системи за дистанционна биометрична идентификация в реално време на обществено достъпни места за правоохранителни цели, освен ако и доколкото такова използване е строго необходимо за една от следните цели:
- i) целево издирване на конкретни жертви на отвличане, трафик на хора и сексуална експлоатация на хора, както и издирване на изчезнали лица;
 - ii) предотвратяване на конкретна, значителна и непосредствена заплаха за живота или физическата безопасност на физически лица или на действителна и настояща или действителна и предвидима заплаха от терористично нападение;
 - iii) установяване на местонахождението или самоличността на лице, заподозряно в извършването на престъпление, за целите на провеждането на разследване или наказателно преследване или на изпълнението на наказание за престъпления, посочени в приложение II и наказуеми в съответната държава членка с лишаване от свобода или мярка за задържане с максимален срок не по-малко от четири години.

Първа алинея, буква з) не засяга член 9 от Регламент (ЕС) 2016/679 за обработването на биометрични данни за цели, различни от правоохранителни цели.

2. Използването на системи за дистанционна биометрична идентификация в реално време на обществено достъпни места за правоохранителни цели за която и да е от целите, посочени в параграф 1, първа алинея, буква з), се извършва за целите, посочени в същата буква, само с оглед на потвърждаването на самоличността на конкретно лице и при отчитане на следните елементи:

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

Освен това използването на системи за дистанционна биометрична идентификация в реално време на обществено достъпни места за правоохранителни цели за някоя от целите, посочени в параграф 1, първа алинея, буква з) от настоящия член, трябва да съответства на необходимите и пропорционални гаранции и условия за използване в съответствие с националното право, което допуска такова използване, и по-специално по отношение на времевите, териториалните ограничения и ограниченията по отношение на лицата. Използването на системи за дистанционна биометрична идентификация в реално време на обществено достъпни места се разрешава само ако правоохранителният орган е извършил оценката на въздействието върху основните права, посочена в член 27, и е регистрирал системата в базата данни на ЕС в съответствие с член 49. В надлежно обосновани спешни случаи обаче използването на тези системи може да започне без регистрация в базата данни на ЕС, при условие че регистрацията бъде извършена без ненужно забавяне.

3. За целите на параграф 1, първа алинея, буква з) и параграф 2, за всяко използване за правоохранителни цели на система за дистанционна биометрична идентификация в реално време на обществено достъпни места се изисква предварително разрешение, което се издава от съдебен орган или от независим административен орган, чието решение е задължително, на държавата членка, в която ще се осъществи използването, след получаване на мотивирано искане и в съответствие с подробните правила на националното право, посочени в параграф 5. В надлежно обосновани спешни случаи обаче използването на системата може да започне без разрешение, при условие че такова разрешение се поиска без ненужно забавяне, най-късно в рамките на 24 часа. Ако искането за разрешение бъде отхвърлено, използването се прекратява незабавно и всички данни, както и резултатите от това използване, незабавно се премахват и заличават.

Компетентният съдебен орган или независим административен орган, чието решение е задължително, издава разрешението само ако въз основа на обективни доказателства или данни за ясни признаци, които са му представени, се убеди, че използването на въпросната система за дистанционна биометрична идентификация в реално време е необходимо и пропорционално за постигането на една от целите, посочени в параграф 1, първа алинея, буква з), която се посочва в искането, и по-специално се ограничава до строго необходимото по отношение на времевия и териториалния обхват

и обхвата по отношение на лицата. Когато взема решение по искането, този орган взема предвид елементите, посочени в параграф 2. Не може да бъде взето решение, пораждащо неблагоприятни правни последици за дадено лице, единствено въз основа на резултата от системата за дистанционна биометрична идентификация в реално време.

4. Без да се засяга параграф 3, за всяко използване на система за дистанционна биометрична идентификация в реално време на обществено достъпни места за правоохранителни цели се уведомяват съответният орган за надзор на пазара и националният орган за защита на данните в съответствие с националните правила, посочени в параграф 5. Уведомлението съдържа най-малко информацията, посочена в параграф 6, и не включва чувствителни оперативни данни.

5. 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 правоохранителни цели в рамките на ограниченията и при условията, изброени в параграф 1, първа алинея, буква з) и в параграфи 2 и 3. Съответните държави членки установяват в националното си право необходимите подробни правила за подаване на искания за разрешенията, посочени в параграф 3, за тяхното издаване и изпълнение, както и за надзора и докладването по отношение на тях. В тези правила се конкретизира също така по отношение на кои от целите, посочени в параграф 1, първа алинея, буква з), включително по отношение на кои престъпления, посочени в буква з), точка iii) от същата разпоредба, на компетентните органи може да бъде разрешено да използват тези системи за правоохранителни цели. Държавите членки съобщават на Комисията тези правила най-късно 30 дни след приемането им. Държавите членки могат да въведат, в съответствие с правото на Съюза, по-ограничителни законови разпоредби относно използването на системи за дистанционна биометрична идентификация.

6. Националните органи за надзор на пазара и националните органи за защита на данните на държавите членки, които са били уведомени за използването на системи за дистанционна биометрична идентификация в реално време на обществено достъпни места за правоохранителни цели съгласно параграф 4, представят на Комисията годишни доклади относно това използване. За тази цел Комисията осигурява на държавите членки и на националните органи за надзор на пазара и за защита на данните образец, включващ информация за броя на решенията, взети от компетентните съдебни органи или от независим административен орган, чието решение е задължително, по отношение на искания за разрешения в съответствие с параграф 3 и за резултатите от тях.

7. Комисията публикува годишни доклади относно използването на системи за дистанционна биометрична идентификация в реално време на обществено достъпни места за правоохранителни цели на базата на обобщени данни в държавите членки, основани на посочените в параграф 6 годишни доклади. Тези годишни доклади не съдържат чувствителни оперативни данни от съответните правоохранителни дейности.

8. Настоящият член не засяга забраните, които се прилагат, когато дадена практика в областта на ИИ нарушава друго право на Съюза.

ГЛАВА III

ВИСОКОРИСКОВИ СИСТЕМИ С ИИ

РАЗДЕЛ 1

Класифициране на системи с ИИ като високорискови

Член 6

Правила за класифициране на системи с ИИ като високорискови

1. Без оглед на това дали дадена система с ИИ се пуска на пазара или се пуска в действие 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 на продукт или самата система с ИИ е продукт, попадащ в обхвата на законодателството на Съюза за хармонизация, посочено в приложение I;
- б) продуктът, чийто защитен елемент съгласно буква а) е системата с ИИ, или самата система с ИИ като продукт трябва да премине оценяване на съответствието от трето лице с оглед на пускането на пазара или пускането в действие на посочения продукт в съответствие със законодателството на Съюза за хармонизация, посочено в приложение I.

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

3. Чрез дерогация от параграф 2, система с ИИ, посочена в приложение III, не се счита за високорискова, ако не представлява значителен риск от увреждане на здравето, безопасността или основните права на физическите лица, включително като не оказва съществено влияние върху резултата от вземането на решения.

Първа алинея се прилага, когато е изпълнено някое от следните условия:

- а) системата с ИИ е предназначена да изпълнява точно формулирана процедурна задача;
- б) системата с ИИ е предназначена да подобри резултата от извършена преди това човешка дейност;
- в) системата с ИИ е предназначена да открива модели за вземане на решения или отклонения от предходни модели за вземане на решения и не е предназначена да замени или повлияе на направената преди това човешка оценка, без да бъде извършен подходящ преглед от човек; или
- г) системата с ИИ е предназначена да изпълнява подготвителна задача с оглед на извършването на оценка, която е от значение за целите на случаите на използване, посочени в приложение III.

Независимо от първа алинея, система с ИИ, посочена в приложение III, винаги се счита за високорискова, когато извършва профилиране на физически лица.

4. Доставчик, който счита, че дадена система с ИИ, посочена в приложение III, не е високорискова, документира своята оценка, преди тази система да бъде пусната на пазара или пусната в действие. За такъв доставчик се прилага задължението за регистрация, установено в член 49, параграф 2. При поискване от националните компетентни органи доставчикът предоставя документацията за оценката.

5. Комисията, след консултация с Европейския съвет по изкуствен интелект (наричан по-долу „Съветът по ИИ“) и не по-късно от 2 февруари 2026 г., дава насоки, с които конкретизира практическото прилагане на настоящия член в съответствие с член 96, заедно с изчерпателен списък с практически примери за случаи на употреба на системи с ИИ, които са високорискови, и такива, които не са високорискови.

6. На Комисията се предоставя правомощието да приема делегирани актове в съответствие с член 97 за изменение на параграф 3, втора алинея от настоящия член чрез добавяне на нови условия към установените в посочената разпоредба или за изменението им, когато има конкретни и достоверни доказателства за наличието на системи с ИИ, които попадат в обхвата на приложение III, но не пораждат значителен риск от увреждане на здравето, безопасността или основните права на физическите лица.

7. Комисията приема делегирани актове в съответствие с член 97 за изменение на параграф 3, втора алинея от настоящия член чрез заличаване на някое от условията, установени в посочената разпоредба, когато има конкретни и достоверни доказателства, че това е необходимо за поддържането на равнището на защита на здравето, безопасността и основните права, предвидено в настоящия регламент.

8. Приетите в съответствие с параграфи 6 и 7 от настоящия член изменения на условията, установени в параграф 3, втора алинея, не може да намаляват общото равнище на защита на здравето, безопасността и основните права, предвидено в настоящия регламент, трябва да осигуряват съгласуваност с делегираните актове, приети съгласно член 7, параграф 1, и да са съобразени с пазарното и технологичното развитие.

Член 7

Изменения на приложение III

1. На Комисията се предоставя правомощието да приема делегирани актове в съответствие с член 97 за изменение на приложение III чрез добавяне на нови или изменение на случаите на употреба на високорискови системи с ИИ, когато са изпълнени следните две условия:

- а) системите с ИИ са предназначени за използване в някоя от областите, посочени в приложение III;
- б) системите с ИИ пораждат риск от увреждане на здравето и безопасността или риск от неблагоприятно въздействие върху основните права и този риск е равностоен или по-голям от риска от увреждане или неблагоприятно въздействие, породен от високорисковите системи с ИИ, които вече са посочени в приложение III.

2. При оценката във връзка с условието по параграф 1, буква б), Комисията взема предвид следните критерии:
- а) предназначението на системата с ИИ;
 - б) степента, в която дадена система с ИИ е била използвана или е вероятно да бъде използвана;
 - в) естеството и количеството на данните, обработвани и използвани от системата с ИИ, и по-специално дали се обработват специални категории лични данни;
 - г) степента, в която системата с ИИ действа автономно, и възможността човек да отхвърли решение или препоръки, които могат да доведат до евентуална вреда;
 - д) степента, в която използването на система с ИИ вече е причинило увреждане на здравето и безопасността или е оказало неблагоприятно въздействие върху основните права, или е породило значителни опасения във връзка с вероятността от такова увреждане или неблагоприятно въздействие, като за това свидетелстват например доклади или документираните твърдения, представени на националните компетентни органи, или други доклади, когато е приложимо;
 - е) потенциалната степен на такова увреждане или неблагоприятно въздействие, по-специално по отношение на неговия интензитет и способността му да засегне множество лица или да засегне несъразмерно конкретна група лица;
 - ж) степента, в която лицата, които може да бъдат засегнати от 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;
 - з) степента, в която съществува властово неравновесие или в която лицата, които може да бъдат засегнати от увреждане или неблагоприятно въздействие, се намират в уязвимо положение по отношение на внедрителя на система с ИИ, по-специално поради статус, авторитет, познания, икономическо или социално положение или възраст;
 - и) степента, в която резултатът, получен с използването на система с ИИ, е лесно поправим или обратим, предвид наличните технически решения за неговата поправка или отхвърляне, при които резултатите, оказващи неблагоприятно въздействие върху здравето, безопасността или основните права, не се считат за лесно поправими или обратими;
 - й) мащаба и вероятната полза от внедряването на системата с ИИ за отделни лица, групи или обществото като цяло, включително възможни подобрения на безопасността на продуктите;
 - к) степента, в която в действащото право на Съюза са предвидени:
 - i) ефективни мерки за правна защита във връзка с рисковете, произтичащи от дадена система с ИИ, с изключение на искове за обезщетение;
 - ii) ефективни мерки за предотвратяване или значително намаляване на тези рискове.
3. На Комисията се предоставя правомощието да приема делегирани актове в съответствие с член 97 за изменение на списъка в приложение III чрез заличаване на високорискови системи с ИИ, когато са изпълнени следните две условия:
- а) съответната високорискова система с ИИ или системи с ИИ вече не поражда(т) значителен риск за основните права, здравето или безопасността предвид критериите, изброени в параграф 2;
 - б) заличаването не намалява общото равнище на защитата на здравето, безопасността и основните права съгласно правото на Съюза.

РАЗДЕЛ 2

Изисквания по отношение на високорисковите системи с ИИ

Член 8

Съответствие с изискванията

1. Високорисковите системи с ИИ трябва да съответстват на изискванията, установени в настоящия раздел, като се взема предвид тяхното предназначение, както и общоприетите съвременни технически постижения в областта на ИИ и свързаните с ИИ технологии. При осигуряването на съответствие с тези изисквания се взема предвид системата за управление на риска, посочена в член 9.

2. Когато даден продукт съдържа система с ИИ, за която се прилагат изискванията на настоящия регламент, както и изискванията на законодателството на Съюза за хармонизация, посочено в раздел А от приложение I, доставчиците носят отговорност за осигуряване на пълното съответствие на продукта с всички приложими изисквания съгласно приложимото законодателство на Съюза за хармонизация. С оглед на осигуряване на съответствието на високорисковите системи с ИИ, посочени в параграф 1, с изискванията, установени в настоящия раздел, и с цел да се осигури съгласуваност, да се избегне дублиране и да се сведе до минимум допълнителната тежест, доставчиците могат да изберат да включат, когато е целесъобразно, необходимите процеси на изпитване и докладване, информация и документация, които предоставят за своя продукт, във вече съществуваща документация и процедури, изисквани съгласно законодателството на Съюза за хармонизация, посочено в раздел А от приложение I.

Член 9

Система за управление на риска

1. Във връзка с високорисковите системи с ИИ се създава, прилага, документира и поддържа система за управление на риска.
2. Системата за управление на риска се разбира като непрекъснат цикличен процес, планиран и протичащ през целия жизнен цикъл на високорисковата система с ИИ и изискващ редовен и систематичен преглед и актуализиране. Тя включва следните стъпки:
 - а) установяване и анализ на известните и разумно предвидимите рискове, които високорисковата система с ИИ може да породии по отношение на здравето, безопасността и основните права, когато високорисковата система с ИИ се използва в съответствие с предназначението си;
 - б) прогноза и оценка на рисковете, които могат да възникнат, когато високорисковата система с ИИ се използва в съответствие с предназначението си и в условия на разумно предвидима неправилна експлоатация;
 - в) оценка на други евентуално възникващи рискове въз основа на анализ на данните, събрани от системата за мониторинг след пускането на пазара, посочена в член 72;
 - г) приемане на подходящи и целенасочени мерки за управление на риска, разработени с цел преодоляване на рисковете, установени съгласно буква а).
3. Рисковете, посочени в настоящия член, се отнасят само до тези, които могат да бъдат разумно ограничени или отстранени при разработването или проектирането на високорисковата система с ИИ или чрез предоставянето на подходяща техническа информация.
4. Мерките за управление на риска, посочени в параграф 2, буква г), трябва да са надлежно съобразени с последиците и възможното взаимодействие в резултат на съчетаното прилагане на изискванията, установени в настоящия раздел, с цел по-ефективното свеждане до минимум на рисковете, като същевременно се постигне подходящ баланс при прилагането на мерките за изпълнение на тези изисквания.
5. Мерките за управление на риска, посочени в параграф 2, буква г), трябва да са такива, че съответният остатъчен риск, свързан с всяка опасност, както и общият остатъчен риск на високорисковите системи с ИИ, да се считат за приемливи.

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

- а) отстраняване или намаляване на рисковете, установени и оценени съгласно параграф 2, доколкото е технически осъществимо, чрез адекватно проектиране и разработване на високорисковата система с ИИ;
- б) когато е целесъобразно, прилагане на адекватни мерки за ограничаване и контрол по отношение на рисковете, които не могат да бъдат отстранени;
- в) предоставяне на необходимата информация съгласно член 13 и, където е целесъобразно, обучение на внедрителите.

С оглед на 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 внедрителя, и предполагаемият контекст, в който системата е предназначена да се използва.

6. Високорисковите системи с ИИ се изпитват с цел набелязване на най-подходящите и целенасочени мерки за управление на риска. Изпитванията трябва да гарантират, че високорисковите системи с ИИ функционират стабилно с оглед на предназначението си и че са в съответствие с изискванията, установени в настоящия раздел.
7. Процедурите за изпитване може да включват изпитване в реални условия в съответствие с член 60.
8. Изпитването на високорисковите системи с ИИ се извършва, когато е целесъобразно, във всеки момент от процеса на разработване и — при всички случаи — преди пускането им на пазара или пускането им в действие. Изпитването се извършва спрямо предварително определени показатели и вероятностни прагове, които са подходящи с оглед на предназначението на високорисковата система с ИИ.
9. При прилагането на системата за управление на риска, предвидена в параграфи 1—7, доставчиците разглеждат въпроса дали, с оглед на предназначението на високорисковата система с ИИ, е вероятно тя да окаже неблагоприятно въздействие върху ненавършили 18 години лица и, в зависимост от случая, върху други уязвими групи.
10. За доставчиците на високорискови системи с ИИ, спрямо които се прилагат изисквания по отношение на вътрешните процеси за управление на риска съгласно други относими разпоредби на правото на Съюза, аспектите, предвидени в параграфи 1—9, могат да бъдат част от процедурите за управление на риска, установени съгласно това право, или да се съчетават с тях.

Член 10

Данни и администриране на данните

1. Високорисковите системи с ИИ, при които се използват техники, свързани с обучение с данни на модели с ИИ, се разработват въз основа на набори от обучителни, валидационни и изпитвателни данни, които отговарят на критериите за качество, посочени в параграфи 2—5, когато се използват такива набори от данни.
2. По отношение на наборите от обучителни, валидационни и изпитвателни данни се прилагат практики за администриране и управление на данните, подходящи с оглед на предназначението на системата с ИИ. Тези практики се отнасят по-специално до:
 - а) съответните проектантски решения;
 - б) процесите на събиране на данни и произхода на данните и в случай на лични данни — първоначалната цел на събирането на данните;
 - в) съответните операции по подготовка на данните, като аотиране, обозначаване, изчистване, актуализиране, обогатяване и агрегиране;
 - г) формулирането на допускания, по-специално по отношение на информацията, която данните следва да измерват и представят;
 - д) оценка на наличието, количеството и годността на необходимите набори от данни;
 - е) преглед с оглед на евентуална предубеденост, която има вероятност да засегне здравето и безопасността на хората, да окаже отрицателно въздействие върху основните права или да доведе до дискриминация, забранена съгласно правото на Съюза, по-специално когато резултатите от данните оказват влияние върху входящите данни за бъдещи операции;
 - ж) подходящи мерки за откриване, предотвратяване и смекчаване на евентуална предубеденост, установена съгласно буква е);
 - з) откриване на съответни пропуски или недостатъци в данните, които възпрепятстват съответствието с настоящия регламент, и на начините за отстраняване на тези пропуски и недостатъци.
3. Наборите от обучителни, валидационни и изпитвателни данни трябва да са подходящи, достатъчно представителни и във възможно най-голяма степен без грешки и пълни с оглед на предназначението на системата. Те трябва да притежават подходящите статистически свойства, включително, когато е приложимо, по отношение на лицата или групите лица, по отношение на които високорисковата система с ИИ е предназначена да се използва. Тези характеристики на наборите от данни могат да са налични на равнището на отделните набори от данни или по отношение на комбинация от тях.
4. Наборите от данни трябва да са съобразени — доколкото това е необходимо с оглед на предназначението — с характеристиките или елементите, характерни за конкретната географска, контекстуална, поведенческа или функционална среда, в която високорисковата система с ИИ е предназначена да бъде използвана.

5. Доколкото това е строго необходимо, за да се гарантира откриване и коригиране на предубеденост във високорисковите системи с ИИ в съответствие с параграф 2, букви е) и ж) от настоящия член, доставчиците на такива системи могат по изключение да обработват специални категории лични данни при спазването на подходящи гаранции за основните права и свободи на физическите лица. Освен разпоредбите, предвидени в регламенти (ЕС) 2016/679 и (ЕС) 2018/1725 и Директива (ЕС) 2016/680, за да може да се извърши такова обработване, трябва да бъдат изпълнени всички посочени по-долу условия:

- а) откриването и коригирането на предубедеността не могат да се осъществят ефективно чрез обработването на други данни, включително синтетични или анонимизирани данни;
 - б) по отношение на специалните категории лични данни се прилагат технически ограничения, свързани с повторното използване на личните данни, както и най-съвременни мерки за сигурност и опазване на неприкосновеността на личния живот, включително псевдонимизация;
 - в) по отношение на специалните категории лични данни се прилагат мерки, с които се гарантира, че обработваните лични данни са обезопасени, защитени, спрямо тях се прилагат подходящи гаранции, включително строг контрол и документиране на достъпа, с цел да се избегне злоупотреба и да се гарантира, че само оправомощени лица имат достъп до тези лични данни със съответните запълнения за спазване на поверителност;
 - г) специалните категории лични данни не се предоставят, не се предават, нито достъпват по друг начин от други лица;
 - д) специалните категории лични данни се заличават, след като предубедеността бъде коригирана или личните данни достигнат края на срока си на съхранение, като се взема предвид по-рано настъпилото от двете събития;
 - е) записите за дейностите по обработване съгласно регламенти (ЕС) 2016/679 и (ЕС) 2018/1725 и Директива (ЕС) 2016/680 включват причините, поради които обработването на специални категории лични данни е било строго необходимо за откриване и коригиране на предубедеността и не било възможно тази цел да се постигне чрез обработване на други данни.
6. При разработването на високорискови системи с ИИ, които не използват техники, включващи обучение на модели с ИИ, параграфи 2—5 се прилагат само за наборите от изпитвателни данни.

Член 11

Техническа документация

1. Техническата документация на дадена високорискова система с ИИ се изготвя, преди тя да бъде пусната на пазара или пусната в действие, и се поддържа актуална.

Техническата документация се изготвя по такъв начин, че да показва, че високорисковата система с ИИ съответства на изискванията, установени в настоящия раздел, и да предоставя на националните компетентни органи и нотифицираните органи цялата необходима информация в ясна и разбираема форма с цел оценяване на съответствието на системата с ИИ с посочените изисквания. Тя съдържа най-малко елементите, установени в приложение IV. МСП, включително новосъздадените предприятия, могат да предоставят по опростен начин елементите на техническата документация, посочени в приложение IV. За тази цел Комисията създава опростен формуляр за техническа документация, съобразен с нуждите на малките предприятия и микропредприятията. Когато МСП, включително новосъздадените предприятия, изберат да предоставят по опростен начин информацията, изисквана съгласно приложение IV, те използват формуляра, посочен в настоящия параграф. Нотифицираните органи приемат формуляра за целите на оценяването на съответствието.

2. Когато се пуска на пазара или пуска в действие високорискова система с ИИ, свързана с продукт, обхванат от законодателството на Съюза за хармонизация, посочено в раздел А от приложение I, се изготвя един набор от техническа документация, съдържаща цялата посочена в параграф 1 информация, както и информацията, изисквана съгласно тези правни актове.

3. На Комисията се предоставя правомощието да приема делегирани актове в съответствие с член 97 за изменение на приложение IV, когато това е необходимо, за да се гарантира, че предвид техническия напредък техническата документация предоставя цялата информация, необходима за оценяване на съответствието на системата с установените в настоящия раздел изисквания.

Член 12

Поддържане на регистри

1. Високорисковите системи с ИИ технически позволяват автоматичното записване на събития (наричано по-долу „записи“) по време на срока на действие на системата.
2. С цел да се гарантира равнище на проследимост на функционирането на високорисковата система с ИИ, което е подходящо с оглед на нейното предназначение, възможностите за създаване на записи позволяват записване на събития, които са от значение за:
 - а) идентифицирането на ситуации, които могат да доведат до това високорисковата система с ИИ да представлява риск по смисъла на член 79, параграф 1 или до съществено изменение;
 - б) улесняването на мониторинга след пускането на пазара, посочен в член 72; и
 - в) мониторинга на функционирането на високорисковите системи с ИИ, посочен в член 26, параграф 5.
3. За високорисковите системи с ИИ, посочени в точка 1, буква а) от приложение III, възможностите за създаване на записи осигуряват най-малко следното:
 - а) записване на времето на всяко използване на системата (начална дата и час и крайна 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) посочване на самоличността на физическите лица, участвали в проверката на резултатите, посочена в член 14, параграф 5.

Член 13

Прозрачност и предоставяне на информация на внедрителите

1. Високорисковите системи с ИИ се проектират и разработват така, че да се гарантира, че функционирането им е достатъчно прозрачно, за да позволи на внедрителите да тълкуват резултатите, получени от системата, и да ги използват по подходящ начин. Осигурява се подходящ вид и степен на прозрачност с оглед изпълнение на приложимите задължения на доставчика и внедрителя, установени в раздел 3.
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 относима, достъпна и разбираема за внедрителите.
3. Инструкциите за употреба съдържат най-малко следната информация:
 - а) идентификационните данни и данните за връзка с доставчика и когато е приложимо, същите данни за неговия упълномощен представител;
 - б) характеристиките, способностите и ограниченията в действието на високорисковата система с ИИ, включително:
 - i) нейното предназначение;
 - ii) нивото на точност, включително използваните за него показатели, на надеждност и на киберсигурност, посочено в член 15, спрямо което е изпитана и валидирана високорисковата система с ИИ и което може да се очаква, както и всички известни или предвидими обстоятелства, които могат да окажат въздействие върху очакваното ниво на точност, надеждност и киберсигурност;
 - iii) всички 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, посочени в член 9, параграф 2;
 - iv) когато е приложимо, техническите способности и характеристики на високорисковата система с ИИ за предоставяне на информация, която е от значение, за да се обяснят резултатите от системата;

- v) когато е целесъобразно, действието ѝ по отношение на конкретни лица или групи лица, спрямо които системата е предназначена да се използва;
 - vi) когато е целесъобразно, спецификациите на входящите данни или всякаква друга относима информация по отношение на използваните набори от обучителни, валидационни и изпитвателни данни, като се отчита предназначението на високорисковата система с ИИ;
 - vii) когато е приложимо, информация, която да позволи на внедрителите да тълкуват резултатите от високорисковата система с ИИ и да ги използват по подходящ начин;
- 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 упражняване на човешки контрол, посочени в член 14, включително техническите мерки, въведени с цел улесняване на тълкуването от страна на внедрителите на резултатите от високорисковите системи с ИИ;
- д) необходимите изчислителни и хардуерни ресурси, очаквания срок на експлоатация на високорисковата система с ИИ и евентуалните необходими мерки за поддръжка и обслужване, включително тяхната честота, с цел да се гарантира правилното функциониране на системата с ИИ, включително по отношение на актуализациите на софтуера;
- е) когато е приложимо, описание на механизмите, включени във високорисковата система с ИИ, които позволяват на внедрителите правилно да събират, съхраняват и тълкуват записите в съответствие с член 12.

Член 14

Човешки контрол

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 контрол от физически лица в периода, през който се използват.
2. Човешкият контрол има за цел предотвратяването или свеждането до минимум на рисковете за здравето, безопасността или основните права, които могат да възникнат при използването на високорискова система с ИИ в съответствие с нейното предназначение или при условия на разумно предвидима неправилна експлоатация, по-специално когато тези рискове продължават да съществуват, независимо от прилагането на останалите изисквания, установени в настоящия раздел.
3. Мерките за контрол трябва да са съразмерни спрямо рисковете, нивото на автономност и контекста на използване на високорисковата система с ИИ и да се осигуряват чрез единия или двата вида мерки, които са посочени по-долу:
 - а) мерки, които са набелязани и вградени, когато това е технически осъществимо, във високорисковата система с ИИ от доставчика преди пускането ѝ на пазара или пускането ѝ в действие;
 - б) мерки, които са набелязани от доставчика преди пускането на високорисковата система с ИИ на пазара или пускането ѝ в действие и които са подходящи за прилагане от страна на внедрителя.
4. За целите на прилагането на параграфи 1, 2 и 3 високорисковата система с ИИ се предоставя на ползвателя по начин, който дава възможност на физическите лица, на които е възложено да упражняват човешки контрол, когато е целесъобразно и пропорционално:
 - а) да разбират добре съответните способности и ограничения на високорисковата система с ИИ и да могат надлежно да следят нейното функциониране, включително с оглед на откриването и справянето с аномалии, отклонения във функционирането и неочаквано действие;
 - б) да осъзнават възможната тенденция автоматично да се разчита или в прекалено голяма степен да се разчита на резултатите, получени от високорискова система с ИИ (т.нар. „предубеденост в полза на автоматизирани решения“), по-специално при високорискови системи с ИИ, използвани за предоставяне на информация или препоръки във връзка с решения, които се вземат от физически лица;
 - в) да тълкуват правилно резултатите от високорисковата система с ИИ, като вземат предвид например наличните инструменти и методи за тълкуване;

- г) да вземат решение — във всяка една конкретна ситуация — да не използват резултата от високорисковата система с ИИ или по друг начин да го пренебрегнат, отхвърлят или отменят;
- д) да се намесят в работата на високорисковата система с ИИ или да прекъснат системата чрез бутон „стоп“ или подобна процедура, която позволява системата да спре в безопасно състояние.

5. За високорисковите системи с ИИ, посочени в точка 1, буква а) от приложение III, мерките, посочени в параграф 3 от настоящия член, трябва да са такива, че освен това да гарантират, че внедрителят не предприема действия, нито взема решения въз основа на идентификацията, получена от системата, освен ако тази идентификация не е била отделно проверена и потвърдена от най-малко две физически лица, притежаващи необходимата компетентност и авторитет и преминали необходимото обучение.

Изискването за отделна проверка от най-малко две физически лица не се прилага за високорискови системи с ИИ, използвани за правоохранителни цели или за целите на миграцията, граничния контрол или убежището, когато правото на Съюза или националното право счита прилагането на това изискване за непропорционално.

Член 15

Точност, надеждност и киберсигурност

1. Високорисковите системи с ИИ се проектират и разработват така, че да постигат подходящо ниво на точност, надеждност и киберсигурност и да функционират стабилно в това отношение в течение на жизнения си цикъл.
2. Във връзка с техническите аспекти на измерването на подходящите равнища на точност и надеждност, посочени в параграф 1, както и на всички други показатели за ефективност, Комисията, в сътрудничество със съответните заинтересовани страни и организации, като например органите по метрология и сравнителен анализ, насърчава, когато е целесъобразно, разработването на сравнителни показатели и методики за измерване.
3. Нивата на точност и съответните показатели за точност на високорисковите системи с ИИ се обявяват в придружаващите ги инструкции за употреба.
4. Високорисковите системи с ИИ трябва да са възможно най-устойчиви по отношение на грешки, недостатъци или несъответствия, които могат да възникнат в рамките на системата или в средата, в която тя работи, по-специално поради взаимодействието им с физически лица или други системи. За тази цел се предприемат технически и организационни мерки.

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 пускането им в действие, се разработват така, че да се отстрани или намали, доколкото е възможно, рискът от евентуално опорочени от предубеденост резултати, оказващи влияние върху входящите данни за бъдещи операции (наричани по-долю „обратни връзки“), и да се гарантира, че спрямо всякакви такива обратни връзки надлежно се вземат подходящи мерки за смекчаване на последиците.

5. Високорисковите системи с ИИ трябва да са устойчиви по отношение на опитите на неоправомощени трети лица да променят използването, резултатите или действието им, като използват уязвимите места на системата.

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

Техническите решения за преодоляване на характерните за ИИ уязвими места включват, когато е целесъобразно, мерки за предотвратяване, откриване, реакция, неутрализиране и контрол на атаки, целящи да манипулират набора от обучителни данни (т.нар. „отравяне на данните“) или предварително обучените компоненти, използвани за обучение (т.нар. „отравяне на моделите“), за предотвратяване на входящи данни, разработени с цел да накарат модела с ИИ да допусне грешка (т.нар. „враждебни примери“ или „заобикаляне на модела“), на атаки срещу поверителността или недостатъци на модела.

РАЗДЕЛ 3

Задължения на доставчиците и внедрителите на високорискови системи с ИИ и на други лица

Член 16

Задължения на доставчиците на високорискови системи с ИИ

Доставчиците на високорискови системи с ИИ:

- а) гарантират, че техните високорискови системи с ИИ съответстват на изискванията, установени в раздел 2;
- б) посочват върху високорисковата система с ИИ, или, когато това не е възможно — върху нейната опаковка или придружаваща документация, в зависимост от случая, своето име, регистрирано търговско наименование или регистрирана търговска марка и адреса си за връзка;
- в) разполагат със система за управление на качеството, която е в съответствие с член 17;
- г) съхраняват документацията, посочена в член 18;
- д) когато са под техен контрол, съхраняват записите, автоматично генерирани от техните високорискови системи с ИИ, посочени в член 19;
- е) гарантират, че високорисковата система с ИИ преминава през съответната процедура за оценяване на съответствието, посочена в член 43, преди да бъде пусната на пазара или пусната в действие;
- ж) изготвят ЕС декларация за съответствие съгласно член 47;
- з) поставят маркировката „СЕ“ върху високорисковата система с ИИ, или, когато това не е възможно — върху нейната опаковка или придружаваща документация, за да укажат съответствието с настоящия регламент, в съответствие с член 48;
- и) изпълняват задълженията за регистрация, посочени в член 49, параграф 1;
- й) предприемат необходимите коригиращи действия и предоставят информацията, изисквана съгласно член 20;
- к) при мотивирано искане на национален компетентен орган доказват съответствието на високорисковата система с ИИ с изискванията, установени в раздел 2;
- л) гарантират, че високорисковата система с ИИ отговаря на изискванията за достъпност в съответствие с директиви (ЕС) 2016/2102 и (ЕС) 2019/882.

Член 17

Система за управление на качеството

1. Доставчиците на високорискови 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 с процедурите за управление на измененията на високорисковата система с ИИ;
- б) техники, процедури и системни действия, които да се използват при проектирането, контрола и проверката на проекта на високорисковата система с ИИ;
- в) техники, процедури и системни действия, които да се използват за разработването, 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 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 или не включват всички съответни изисквания, установени в раздел 2 —средствата, които трябва да се използват с цел да се гарантира, че високорисковата система с ИИ съответства на тези изисквания;
- е) системи и процедури за управление на данни, включително придобиване, събиране, анализ, обозначаване, 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 пускането в действие 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 пускането на пазара в съответствие с член 72;
- и) процедури, свързани с докладването на сериозен инцидент в съответствие с член 73;
- й) провеждането на комуникацията с националните компетентни органи, други съответни органи, включително тези, осигуряващи или съдействащи за достъпа до данни, нотифицираните органи, другите оператори, потребителите или други заинтересовани лица;
- к) системи и процедури за регистриране на цялата относима 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. Прилагането на аспектите, посочени в параграф 1, трябва да е пропорционално на размера на организацията на доставчика. При всички случаи доставчиците спазват степента на вискателност и равнището на защита, необходими за осигуряване на съответствието на техните системи с ИИ с настоящия регламент.

3. За доставчиците на високорискови системи с ИИ, за които се прилагат задължения по отношение на системите за управление на качеството или равностойна функция съгласно съответното секторно право на Съюза, аспектите, посочени в параграф 1, могат да бъдат част от системите за управление на качеството съгласно това право.

4. За доставчиците, които са финансови институции, за които се прилагат изисквания по отношение на тяхното вътрешно управление, мерки или процеси съгласно правото на Съюза в областта на финансовите услуги, задължението за въвеждане на система за управление на качеството, с изключение на параграф 1, букви ж), з) и и) от настоящия член, се счита за изпълнено при наличие на съответствие с правилата за вътрешно управление, мерки или процеси съгласно съответното право на Съюза в областта на финансовите услуги. За тази цел се вземат предвид евентуалните хармонизирани стандарти, посочени в член 40.

Член 18

Съхранение на документация

1. В продължение на 10 години след пускането на пазара или пускането в действие на високорисковата система с ИИ доставчикът съхранява на разположение на националните компетентни органи:

- а) техническата документация, посочена в член 11;
- б) документацията, свързана със системата за управление на качеството, посочена в член 17;
- в) когато е приложимо, документацията относно промените, одобрени от нотифицираните органи;
- г) когато е приложимо, решенията и другите документи, изготвени от нотифицираните органи;
- д) ЕС декларацията за съответствие, посочена в член 47.

2. Всяка държава членка определя условията, при които документацията, посочена в параграф 1, остава на разположение на националните компетентни органи за срока, посочен в същия параграф, за случаите, когато доставчик или негов упълномощен представител, установен на нейна територия, изпадне в несъстоятелност или прекрати дейността си преди изтичането на този срок.

3. Доставчиците, които са финансови институции, спрямо които се прилагат изисквания по отношение на тяхното вътрешно управление, мерки или процеси съгласно правото на Съюза в областта на финансовите услуги, поддържат техническата документация като част от документацията, съхранявана съгласно съответното право на Съюза в областта на финансовите услуги.

Член 19

Автоматично генерирани записи

1. Доставчиците на високорискови системи с ИИ съхраняват записите, посочени в член 12, параграф 1, които са автоматично генерирани от техните високорискови системи с ИИ, доколкото тези записи са под техен контрол. Без да се засяга приложимото право на Съюза или национално право, записите се съхраняват за срок, съобразен с предназначението на високорисковата система с ИИ, който е най-малко шест месеца, освен ако не е предвидено друго в приложимото право на Съюза или национално право, по-специално в правото на Съюза относно защитата на личните данни.

2. Доставчиците, които са финансови институции, за които се прилагат изисквания по отношение на тяхното вътрешно управление, мерки или процеси съгласно правото на Съюза в областта на финансовите услуги, поддържат записите, автоматично генерирани от техните високорискови системи с ИИ, като част от документацията, съхранявана съгласно съответното право в областта на финансовите услуги.

Член 20

Коригиращи действия и задължение за предоставяне на информация

1. 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 пуснали в действие, не съответства на настоящия регламент, незабавно предприемат необходимите коригиращи действия, за да приведат системата в съответствие, да я изтеглят, да я блокират или да я изземат, в зависимост от случая. Те информират съответно дистрибуторите на съответната високорискова система с ИИ и, ако е приложимо, внедрителите, упълномощения представител и вносителите.

2. Когато високорисковата система с ИИ представлява риск по смисъла на член 79, параграф 1 и този риск стане известен на доставчика, той незабавно разследва причините, когато е приложимо — в сътрудничество с уведомялия го внедрител — и уведомява органите за надзор на пазара, които са компетентни по отношение на високорисковата система с ИИ, както и, когато е приложимо — нотифицирания орган, издал сертификат за тази високорискова система с ИИ в съответствие с член 44, по-специално за естеството на несъответствието и за евентуалните предприети коригиращи действия.

Член 21

Сътрудничество с компетентните органи

1. При мотивирано искане от страна на компетентен орган доставчиците на високорискови системи с ИИ предоставят на този орган цялата информация и документация, необходими за доказване на съответствието на високорисковата система с ИИ с изискванията, установени в раздел 2, на един от официалните езици на институциите на Съюза, посочен от съответната държава членка, който може да бъде лесно разбран от органа.

2. Освен това при мотивирано искане от страна на компетентен орган доставчиците предоставят на отпразилото искането компетентен орган, в зависимост от случая, достъп до записите, автоматично генерирани от високорисковата система с ИИ, посочени в член 12, параграф 1, доколкото тези записи са под техен контрол.

3. Всяка информация, получена от компетентен орган съгласно настоящия член, се третира в съответствие със задълженията за поверителност, установени в член 78.

Член 22

Упълномощени представители на доставчиците на високорискови системи с ИИ

1. Преди да предоставят на пазара на Съюза своите системи с ИИ, доставчиците, установени в трети държави, определят с писмено пълномощно упълномощен представител, който е установен в Съюза.
2. Доставчикът осигурява възможност на упълномощения си представител да изпълнява задачите, посочени в пълномощното, получено от доставчика.
3. Упълномощеният представител изпълнява задачите, посочени в пълномощното, получено от доставчика. При поискване той предоставя на органите за надзор на пазара копие от пълномощното на един от официалните езици на институциите на Съюза, посочен от компетентния орган. За целите на настоящия регламент пълномощното дава право на упълномощения представител да изпълнява следните задачи:
 - а) да проверява дали ЕС декларацията за съответствие, посочена в член 47, и техническата документация, посочена в член 11, са изготвени и дали е проведена подходяща процедура за оценяване на съответствието от страна на доставчика;
 - б) да съхранява на разположение на компетентните органи и националните органи, посочени в член 74, параграф 10, в продължение на 10 години след пускането на пазара или пускането в действие на високорисковата система с ИИ данните за контакт на доставчика, който е определил упълномощения представител, копие от ЕС декларацията за съответствие, посочена в член 47, техническата документация и, ако е приложимо, сертификата, издаден от нотифицирания орган;
 - в) при мотивирано искане да предоставя на компетентния орган цялата информация и документация, включително посочената в буква б) от настоящата алинея, която е необходима за доказване на съответствието на дадена високорискова система с ИИ с изискванията, установени в раздел 2, включително достъп до записите, посочени в член 12, параграф 1, които са генерирани автоматично от високорисковата система с ИИ, доколкото тези записи са под контрола на доставчика;
 - г) при мотивирано искане да си сътрудничи с компетентните органи при евентуални действия, предприемани от тях във връзка с високорисковата система с ИИ, по-специално за намаляване и смекчаване на рисковете, породени от високорисковата система с ИИ;
 - д) когато е приложимо, да изпълнява задълженията за регистрация, посочени в член 49, параграф 1, или ако регистрацията се извършва от самия доставчик, да гарантира, че информацията, посочена в раздел А, точка 3 от приложение VIII, е вярна.

Пълномощното дава право на упълномощения представител да отговаря, наред или вместо доставчика, пред компетентните органи по всички въпроси, свързани с осигуряването на съответствие с настоящия регламент.

4. Упълномощеният представител се отказва от упълномощаването, ако счита или има основание да счита, че доставчикът действа в противоречие със задълженията си съгласно настоящия регламент. В такъв случай той също така незабавно информира съответния орган за надзор на пазара, както и, когато е приложимо, съответния нотифициран орган, за отказа от упълномощаването и основанията за това.

Член 23

Задължения на вносителите

1. Преди да пуснат на пазара високорискова система с ИИ, вносителите гарантират, че системата е в съответствие с настоящия регламент, като се уверяват, че:
 - а) съответната процедура за оценяване на съответствието, посочена в член 43, е била проведена от доставчика на високорисковата система с ИИ;
 - б) доставчикът е изготвил техническата документация в съответствие с член 11 и приложение IV;
 - в) системата е означена с изискваната маркировка „СЕ“ и е придружена от ЕС декларацията за съответствие, посочена в член 47, и инструкциите за употреба;
 - г) доставчикът е определил упълномощен представител в съответствие с член 22, параграф 1.

2. Когато вносител има основателна причина да счита, че дадена високорискова система с ИИ не е в съответствие с настоящия регламент или е подправена или придружена от подправена документация, 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 79, параграф 1, вносителят уведомява за това доставчика на системата, упълномощения представител и органите за надзор на пазара.
3. Вносителите посочват своето име, регистрирано търговско наименование или регистрирана търговска марка и адреса си за връзка върху високорисковата система с ИИ, върху нейната опаковка или придружавашата документация, когато е приложимо.
4. Вносителите гарантират, че докато отговарят за дадена високорискова система с ИИ, условията на съхранение или транспортиране, когато е приложимо, не застрашават съответствието ѝ с изискванията, установени в раздел 2.
5. Вносителите съхраняват в продължение на 10 години след пускането на пазара или пускането в действие на високорисковата система с ИИ копие от сертификата, издаден от нотифицирания орган, когато е приложимо, от инструкциите за употреба и от ЕС декларацията за съответствие, посочена в член 47.
6. При мотивирано искане вносителите предоставят на съответните компетентни органи цялата информация и документация, включително посочената в параграф 5, която е необходима за доказване на съответствието на високорискова система с ИИ с изискванията, установени в раздел 2, на език, който може лесно да бъде разбран от тях. За тази цел те също така гарантират, че техническата документация може да бъде предоставена на посочените органи.
7. Вносителите си сътрудничат със съответните компетентни органи при всяко действие, което тези органи предприемат във връзка с високорискова система с ИИ, която вносителите са пуснали на пазара, по-специално за намаляване и смекчаване на породените от нея рискове.

Член 24

Задължения на дистрибуторите

1. Преди да предоставят високорискова система с ИИ на пазара, дистрибуторите се уверяват, че върху нея е нанесена изискваната маркировка „СЕ“, че е придружена от копие от ЕС декларацията за съответствие, посочена в член 47, и от инструкциите за употреба и че доставчикът и вносителят на системата, в зависимост от случая, са изпълнили своите съответни задължения, установени в член 16, букви б) и в) и член 23, параграф 3.
2. Когато дистрибутор счита или има основание да счита, въз основа на информацията, с която разполага, че дадена високорискова система с ИИ не е в съответствие с изискванията, установени в раздел 2, той не предоставя високорисковата система с ИИ на пазара, преди тя да бъде приведена в съответствие с тези изисквания. Освен това, когато високорисковата система с ИИ представлява риск по смисъла на член 79, параграф 1, дистрибуторът уведомява за това доставчика или вносителя на системата, в зависимост от случая.
3. Дистрибуторите гарантират, че докато отговарят за дадена високорискова система с ИИ, условията на съхранение или транспортиране, когато е приложимо, не застрашават съответствието на системата с изискванията, установени в раздел 2.
4. Дистрибутор, който счита или има основание да счита, въз основа на информацията, с която разполага, че дадена високорискова система с ИИ, която е предоставил на пазара, не е в съответствие с изискванията, установени в раздел 2, предприема необходимите коригиращи действия за привеждането ѝ в съответствие с посочените изисквания, за изтеглянето или изнемането ѝ или гарантира, че доставчикът, вносителят или всеки имащ отношение оператор, в зависимост от случая, предприема посочените коригиращи действия. Когато високорисковата система с ИИ представлява риск по смисъла на член 79, параграф 1, дистрибуторът незабавно уведомява за това доставчика или вносителя на системата и органите, които са компетентни по отношение на съответната високорискова система с ИИ, като предоставя подробни данни, по-специално за несъответствието и за евентуалните предприети коригиращи действия.
5. При обосновано искане от съответен компетентен орган дистрибуторите на високорискова система с ИИ предоставят на този орган цялата информация и документация относно своите действия съгласно параграфи 1 – 4, необходими за доказване на съответствието на тази система с изискванията, установени в раздел 2.
6. Дистрибуторите си сътрудничат със съответните компетентни органи при всяко действие, което тези органи предприемат във връзка с високорискова система с ИИ, която дистрибуторите са предоставили на пазара, по-специално за намаляване или смекчаване на породения от нея риск.

Член 25

Отговорности по веригата за създаване на стойност в областта на ИИ

1. Всеки дистрибутор, вносител, внедрител или друго трето лице се счита за доставчик на високорискова система с ИИ за целите на настоящия регламент и за него се прилагат задълженията на доставчика съгласно член 16 в следните случаи:

- а) лицето поставя името или търговската си марка върху високорискова система с ИИ, която вече е пусната на пазара или пусната в действие, без да се засягат договорености, предвиждащи, че задълженията се разпределят по друг начин;
- б) лицето въвежда съществено изменение във високорискова система за ИИ, която вече е пусната на пазара или вече е пусната в действие, по такъв начин, че тя продължава да бъде високорискова система с ИИ съгласно член 6;
- в) лицето изменя предназначението на система с ИИ, включително система с ИИ с общо предназначение, която не е класифицирана като високорискова и вече е била пусната на пазара или пусната в действие, по такъв начин, че съответната система с ИИ става високорискова система с ИИ съгласно член 6.

2. При настъпване на обстоятелствата, посочени в параграф 1, доставчикът, който първоначално е пуснал на пазара системата с ИИ или я е пуснал в действие, повече не се счита за доставчик на тази конкретна система с ИИ за целите на настоящия регламент. Първоначалният доставчик си сътрудничи тясно с новите доставчици и предоставя необходимата информация и осигурява разумно очаквания технически достъп и друга помощ, необходими за изпълнението на задълженията, установени в настоящия регламент, по-специално по отношение на оценяването на съответствието на високорисковите системи с ИИ. Настоящият параграф не се прилага в случаите, когато първоначалният доставчик ясно е посочил, че неговата система с ИИ не трябва да бъде променяна във високорискова система с ИИ и следователно за него не възниква задължението за предоставяне на документацията.

3. При високорискови системи с ИИ, които са защитни елементи на продукти, обхванати от законодателството на Съюза за хармонизация, посочено в раздел А от приложение I, производителят на продукти се счита за доставчик на високорисковата система с ИИ и за него се прилагат задълженията по член 16 при някои от следните обстоятелства:

- а) високорисковата система с ИИ се пуска на пазара заедно с продукта с името или търговската марка на производителя на продукта;
- б) високорисковата система с ИИ се пуска в действие с името или търговската марка на производителя на продукта, след като продуктът е бил пуснат на пазара.

4. Доставчикът на високорискова система с ИИ и третото лице, което доставя система с ИИ, инструменти, услуги, компоненти или процеси, които се използват или са интегрирани във високорискова система с ИИ, посочват с писмено споразумение необходимата информация, възможности, технически достъп и друга помощ въз основа на общоприетите съвременни технически постижения, за да може доставчикът на високорисковата система с ИИ да изпълни изцяло задълженията по настоящия регламент. Настоящият параграф не се прилага за трети лица, които предоставят публичен достъп до инструменти, услуги, процеси или компоненти, различни от моделите на ИИ с общо предназначение, с безплатен лиценз с отворен код.

Службата по ИИ може да разработи и препоръча незадължителни примерни условия за договори между доставчиците на високорискови системи с ИИ и трети лица, предоставящи инструменти, услуги, компоненти или процеси, които се използват или са интегрирани във високорискови системи с ИИ. При разработването на незадължителни примерни условия Службата по ИИ взема предвид възможните договорни изисквания, приложими в конкретни сектори или дейности. Незадължителните примерни условия се публикуват и се предоставят на разположение безплатно, в лесно използваем електронен формат.

5. Параграфи 2 и 3 не засягат необходимостта от закрила и защита на правата върху интелектуалната собственост, поверителната търговска информация и търговските тайни в съответствие с правото на Съюза и националното право.

Член 26

Задължения на внедрителите на високорискови системи с ИИ

1. Внедрителите на високорискови системи с ИИ предприемат подходящи технически и организационни мерки, за да гарантират, че използват тези системи в съответствие с придружаващите ги инструкции за употреба съгласно параграфи 3 и 6.

2. Внедрителите възлагат упражняването на човешки контрол на физически лица, които имат необходимата компетентност и авторитет и са преминали необходимото обучение, както и се ползват с необходимата подкрепа.

3. Задълженията, установени в параграфи 1 и 2, не засягат други задължения на внедрителите съгласно правото на Съюза или националното право и свободата на внедрителите да организират собствените си ресурси и дейности с цел изпълнение на мерките за упражняване на човешки контрол, посочени от доставчика.

4. Без да се засягат параграфи 1 и 2, доколкото внедрителят упражнява контрол върху входящите данни, той гарантира, че тези входящи данни са подходящи и достатъчно представителни с оглед на предназначението на високорисковата система с ИИ.

5. Внедрителите наблюдават функционирането на високорисковата система с ИИ въз основа на инструкциите за употреба и, когато е необходимо, уведомяват доставчиците в съответствие с член 72. Когато внедрителите имат основание да считат, че в резултат от използването на високорисковата система с ИИ в съответствие с инструкциите тази система на ИИ може да породи риск по смисъла на член 79, параграф 1, те информират без ненужно забавяне доставчика или дистрибутора и съответния орган за надзор на пазара и спират използването на системата. При установяване на сериозен инцидент внедрителите също така незабавно информират за този инцидент първо доставчика, а след това вносителя или дистрибутора и съответните органи за надзор на пазара. В случай че внедрителят не може да се свърже с доставчика, член 73 се прилага *mutatis mutandis*. Това задължение не обхваща чувствителни оперативни данни на внедрителите на системи с ИИ, които са правоохранителни органи.

За внедрителите, които са финансови институции, спрямо които се прилагат изисквания по отношение на тяхното вътрешно управление, мерки или процеси съгласно правото на Съюза в областта на финансовите услуги, задължението за мониторинг, установено в първа алинея, се счита за изпълнено чрез съответствието с правилата за мерките за вътрешно управление, процесите и механизмите съгласно съответното право в областта на финансовите услуги.

6. Внедрителите на високорискови системи с ИИ съхраняват записите, генерирани автоматично от високорисковата система с ИИ, доколкото тези записи са под техен контрол, за срок, който е съобразен с предназначението на високорисковата система с ИИ и който е най-малко шест месеца, освен ако в приложимото право на Съюза или национално право, по-специално в правото на Съюза относно защитата на личните данни, не е предвидено друго.

Внедрителите, които са финансови институции, спрямо които се прилагат изисквания по отношение на тяхното вътрешно управление, мерки или процеси съгласно правото на Съюза в областта на финансовите услуги, поддържат записите като част от документацията, съхранявана съгласно съответното право на Съюза в областта на финансовите услуги.

7. Преди пускането в действие или използването на високорискова система с ИИ на работното място внедрителите, които са работодатели, информират представителите на работниците и засегнатите работници, че спрямо тях се използва високорисковата система с ИИ. Тази информация се предоставя, когато е приложимо, в съответствие с правилата и процедурите, установени в правото на Съюза и националното право и практика относно информирането на работниците и техните представители.

8. Внедрителите на високорискови системи с ИИ, които са публични органи или институции, органи, служби или агенции на Съюза, спазват задълженията за регистрация, посочени в член 49. Когато внедрителите установят, че високорисковата система с ИИ, която възнамеряват да използват, не е регистрирана в базата данни на ЕС, посочена в член 71, те не използват тази система и информират за това доставчика или дистрибутора.

9. Когато е приложимо, внедрителите на високорискови системи с ИИ използват информацията, предоставена съгласно член 13 от настоящия регламент, за да спазят 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.

10. Без да се засяга Директива (ЕС) 2016/680, в рамките на разследване за целево издирване на лице, което е заподозряно или осъдено за извършването на престъпление, внедрителят на високорискова система с ИИ за последваща дистанционна биометрична идентификация иска -предварително или без ненужно забавяне и след не повече от 48 часа - разрешение за използването на тази система от съдебен орган или административен орган, чието решение е обвързващо и подлежи на съдебен контрол, освен когато системата се използва за първоначално идентифициране на възможен заподозрян въз основа на обективни и проверими факти, които са пряко свързани с престъплението. Всяко използване се ограничава до строго необходимото за разследването на конкретно престъпление.

Ако разрешението, поискано съгласно първа алинея, бъде отказано, използването на системата за последваща дистанционна биометрична идентификация, свързана с исканото разрешение, се спира незабавно и личните данни, свързани с използването на високорисковата система с ИИ, за която е поискано разрешение, се заличават.

Високорисковата система с ИИ за последваща дистанционна биометрична идентификация в никакъв случай не се използва за правоохранителни цели по нецеленасочен начин, без да е налице връзка с престъпление, наказателно производство, действителна и настояща или действителна и предвидима заплаха от престъпление или издирване на конкретно изчезнало лице. Трябва да се гарантира, че правоохранителните органи не могат да вземат решение, пораждащо неблагоприятни правни последици за дадено лице, единствено въз основа на резултата от тези системи за последваща дистанционна биометрична идентификация.

Настоящият параграф не засяга член 9 от Регламент (ЕС) 2016/679 и член 10 от Директива (ЕС) 2016/680 относно обработването на биометрични данни.

Независимо от целта или внедрителя, всяко използване на такива високорискови системи с ИИ се документира в съответната полицейска преписка и се предоставя на съответния орган за надзор на пазара и на националния орган за защита на данните при поискване, като при това се изключва разкриването на чувствителни оперативни данни, свързани с правоохранителната дейност. Настоящата алинея не засяга правомощията, предоставени на надзорните органи съгласно Директива (ЕС) 2016/680.

Внедрителите представят на съответните органи за надзор на пазара и на националните органи за защита на данните годишни доклади относно използването от своя страна на системи за последваща дистанционна биометрична идентификация, като при това се изключва разкриването на чувствителни оперативни данни, свързани с правоохранителната дейност. Докладите могат да бъдат обобщени, за да обхванат повече от едно внедряване.

Държавите членки могат да въведат, в съответствие с правото на Съюза, по-ограничителни законови разпоредби относно използването на системи за последваща дистанционна биометрична идентификация.

11. Без да се засяга член 50 от настоящия регламент, внедрителите на високорискови системи с ИИ, посочени в приложение III, които вземат решения или подпомагат вземането на решения, свързани с физически лица, информират тези лица, че спрямо тях се използва високорискова система с ИИ. За високорисковите системи с ИИ, използвани за правоохранителни цели, се прилага член 13 от Директива (ЕС) 2016/680.

12. Внедрителите си сътрудничат със съответните компетентни органи при всяко действие, предприето от тези органи във връзка с високорисковата система с ИИ, за да приложат настоящия регламент.

Член 27

Оценка на въздействието върху основните права за високорискови системи с ИИ

1. Преди внедряването на високорискова система с ИИ, посочена в член 6, параграф 2, с изключение на високорисковите системи с ИИ, предназначени да бъдат използвани в областта, посочена в точка 2 от приложение III, внедрителите, които са публични органи или са частни субекти, предоставящи публични услуги, и внедрителите на високорисковите системи с ИИ, посочени в точка 5, букви б) и в) от приложение III, извършват оценка на въздействието върху основните права, което може да възникне при използването на такава система. За тази цел внедрителите извършват оценка, която се състои от:

- а) описание на процесите на внедрителя, в които ще се използва високорисковата система с ИИ според нейното предназначение;
- б) посочване на срока, в рамките на който е предназначена за използване високорисковата система с ИИ, и честотата, с която е предназначена да се използва;
- в) категориите физически лица и групи, които е вероятно да бъдат засегнати от използването в конкретния контекст;
- г) конкретните рискове от настъпване на вреди, които е вероятно да окажат въздействие върху категориите лица или групи лица, определени съгласно буква в) от настоящия параграф, като се взема предвид информацията, предоставена от доставчика съгласно член 13;
- д) описание на изпълнението на мерките за упражняване на човешки контрол съгласно инструкциите за употреба;
- е) мерките, които трябва да се предприемат, ако тези рискове се проявят, включително мерките за вътрешно управление и механизмите за подаване на жалби.

2. Задължението, посочено в параграф 1, се прилага за първото използване на високорисковата система с ИИ. В подобни случаи внедрителят може да разчита на предварително извършени оценки на въздействието върху основните права или на съществуващи оценки на въздействието, извършени от доставчика. Ако по време на използването на високорисковата система с ИИ внедрителят прецени, че някой от елементите, изброени в параграф 1, е променен или вече не е актуален, той предприема необходимите стъпки за актуализиране на информацията.
3. След извършването на оценката, посочена в параграф 1 от настоящия член, внедрителят уведомява органа за надзор на пазара за резултатите от нея, като подава попълнен образец, посочен в параграф 5 от настоящия член, като част от уведомлението. В случая, посочен в член 46, параграф 1, внедрителите могат да бъдат освободени от задължението за уведомяване.
4. Ако някое от задълженията, предвидени в настоящия член, вече е изпълнено чрез извършването на оценката на въздействието върху защитата на данните по член 35 от Регламент (ЕС) 2016/679 или член 27 от Директива (ЕС) 2016/680, оценката на въздействието върху основните права, посочена в параграф 1 от настоящия член, допълва тази оценка на въздействието върху защитата на данните.
5. Службата по ИИ разработва образец на въпросник, включително основан на автоматизиран инструмент, за да улесни внедрителите при изпълнението на задълженията по настоящия член по опростен начин.

РАЗДЕЛ 4

Нотифициращи органи и нотифицирани органи

Член 28

Нотифициращи органи

1. Всяка държава членка определя или създава най-малко един нотифициращ орган, който отговаря за въвеждането и извършването на процедурите, необходими за оценяването, определянето и нотифицирането на органи за оценяване на съответствието и за провеждането на мониторинг по отношение на тях. Тези процедури се разработват в сътрудничество между нотифициращите органи на всички държави членки.
2. Държавите членки могат да решат, че оценяването и мониторингът, посочени в параграф 1, се извършват от национален орган по акредитация по смисъла на Регламент (ЕО) № 765/2008 и в съответствие с него.
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 предлагат и не извършват никаква дейност, извършвани от органите за оценяване на съответствието, нито предоставят консултантски услуги с търговска цел или на конкурентна основа.
6. Нотифициращите органи гарантират поверителността на информацията, която получават в съответствие с член 78.
7. Нотифициращите органи трябва да разполагат с достатъчен на брой компетентен персонал, необходим за правилното изпълнение на техните задачи. Компетентният персонал трябва да разполага с необходимия експертен опит, когато е приложимо, за да изпълнява функциите си в области като информационните технологии, ИИ и правото, включително надзора във връзка с основните права.

Член 29

Заявление за нотифициране от орган 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, модула или модулите за оценяване на съответствието и видовете системи с ИИ, 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 31.

Добавят се и всякакви действителни документи, отнасящи се до определянето на подалия заявлението нотифициран орган съгласно друго законодателство на Съюза за хармонизация.

3. Когато органът за оценяване на съответствието не може да представи сертификат за акредитация, той представя пред нотифициращия орган всички удостоверителни документи, необходими за проверката, признаването и редовния мониторинг на спазването от негова страна на изискванията, предвидени в член 31.

4. За нотифицирани органи, които са определени съгласно друго законодателство на Съюза за хармонизация, всички документи и сертификати, свързани с това определяне, могат да се използват в подкрепа на процедурата за тяхното определяне съгласно настоящия регламент, както е целесъобразно. Нотифициращият орган актуализира документацията, посочена в параграфи 2 и 3 от настоящия член, при настъпване на съответните промени, за да се даде възможност на органа, отговарящ за нотифицираните органи, да наблюдава и проверява непрекъснатото съответствие с всички изисквания, предвидени в член 31.

Член 30

Процедура по нотифициране

1. Нотифициращите органи могат да нотифицират само органи за оценяване на съответствието, които отговарят на изискванията, предвидени в член 31.

2. Нотифициращите органи нотифицират Комисията и другите държави членки, като използват инструмента за електронно нотифициране, създаден и поддържан от Комисията, за всеки орган за оценяване на съответствието, посочен в параграф 1.

3. Нотифицирането, посочено в параграф 2 от настоящия член, включва пълни подробности за дейностите по оценяване на съответствието, модула или модулите за оценяване на съответствието, съответните видове системи с ИИ, както и съответното удостоверение за компетентност. Когато нотифицирането не се основава на сертификат за акредитация съгласно член 29, параграф 2, нотифициращият орган предоставя на Комисията и на другите държави членки документи, които удостоверяват компетентността на органа за оценяване на съответствието и съществуващите механизми, с които се гарантира, че този орган ще бъде редовно наблюдаван и ще продължи да отговаря на изискванията, предвидени в член 31.

4. Съответният орган за оценяване на съответствието може да изпълнява дейностите на нотифициран орган само когато Комисията или другите държави членки не са повдигнали възражения в срок от две седмици след нотифицирането от страна на нотифициращия орган, когато това включва сертификат за акредитация съгласно член 29, параграф 2, или в срок от два месеца след нотифицирането от страна на нотифициращия орган, когато това включва удостоверителни документи съгласно член 29, параграф 3.

5. Когато бъдат повдигнати възражения, Комисията без забавяне започва консултации със съответните държави членки и органа за оценяване на съответствието. С оглед на това Комисията решава дали разрешението е обосновано. Комисията адресира решението си до съответната държава членка и съответния орган за оценяване на съответствието.

Член 31

Изисквания, свързани с нотифицираните органи

1. Нотифициращият орган се създава съгласно националното право на дадена държава членка и има правосубектност.

2. Нотифицираните органи трябва да отговарят на организационните изисквания, изискванията за управление на качеството, изискванията във връзка с ресурсите и процесите, необходими за изпълнението на техните задачи, както и на подходящите изисквания за киберсигурност.

3. Организационната структура, разпределението на отговорностите, йерархичната структура и функционирането на нотифицираните органи трябва да гарантират доверие в тяхната работа и в резултатите от дейностите по оценяване на съответствието, които нотифицираните органи извършват.

4. Нотифицираните органи са независими от доставчика на високорисковите системи с ИИ, по отношение на които извършват дейности по оценяване на съответствието. Нотифицираните органи са независими и от всеки друг оператор, който има икономически интерес от високорисковите системи с ИИ, които се оценяват, както и от евентуални конкуренти на доставчика. Това не изключва използването на оценени високорискови системи с ИИ, които са необходими за дейностите на органа за оценяване на съответствието, или използването на такива системи за собствени цели.
5. Органът за оценяване на съответствието, неговите висши ръководители и членове на персонала, отговорни за изпълнение на задачите му по оценяване на съответствието, не вземат пряко участие в проектирането, разработването, предлагането на пазара или използването на високорискови системи с ИИ, нито представляват лицата, участващи в такива дейности. Те не участват в никаква дейност, която би могла да е в противоречие с тяхната независима преценка и почтено поведение по отношение на дейностите по оценяване на съответствието, за които са нотифицирани. Това се прилага по-специално за консултантски услуги.
6. Нотифицираните органи се организират и функционират по начин, който да гарантира независимостта, обективността и безпристрастността на техните дейности. Нотифицираните органи документират и въвеждат структура и процедури за гарантиране на безпристрастност и за насърчване и прилагане на принципите на безпристрастност в цялата си организация, сред целия си персонал и в дейностите си по оценяване.
7. Нотифицираните органи трябва да имат документирани процедури, които гарантират, че техният персонал, комитети, дъщерни дружества, подизпълнители или други свързани органи или персонал на външни органи запазват, в съответствие с член 78, поверителността на информацията, получена при изпълнението на дейностите по оценяване на съответствието, освен когато нейното разкриване се изисква по закон. Персоналът на нотифицираните органи е длъжен да пази служебна тайна по отношение на цялата информация, получена при изпълнение на задачите по настоящия регламент, освен по отношение на нотифициращите органи на държавата членка, в която осъществява дейността си.
8. Нотифицираните органи трябва да разполагат с процедури за изпълнение на дейностите си, са които надлежно съобразени с размера на доставчика, сектора му на дейност, неговата структура и степента на сложност на съответната система с ИИ.
9. Нотифицираните органи сключват подходяща застраховка за покриване на отговорността във връзка с дейностите си по оценяване на съответствието, освен когато отговорността се поема от държавата членка, в която са установени в съответствие с националното право, или когато тази държава членка е пряко отговорна за оценяването на съответствието.
10. Нотифицираните органи трябва да са в състояние 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 под техен контрол.
11. Нотифицираните органи разполагат с достатъчна собствена компетентност, за да могат ефективно да оценяват задачите, изпълнявани от външни лица от тяхно име. Нотифицираният орган разполага с постоянна наличност от достатъчен административен, технически, правен и научен персонал, който притежава опит и знания, свързани със съответните видове системи с ИИ, данни и изчисления на данни, и с изискванията, установени в раздел 2.
12. Нотифицираните органи участват в координационни дейности съгласно 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.

Член 32

Презумпция за съответствие с изискванията, свързани с нотифицираните органи

Когато органът за оценяване на съответствието докаже своето съответствие с критериите, предвидени в съответните хармонизирани стандарти или части от тях, справочната информация за които е била публикувана в *Официален вестник на Европейския съюз*, се смята, че той съответства на изискванията, установени в член 31, доколкото приложимите хармонизирани стандарти обхващат тези изисквания.

Член 33

Използване на подизпълнители и дъщерни дружества от страна на нотифицираните органи

1. В случаите, в които нотифициран орган възлага на подизпълнители конкретни задачи, свързани с оценяване на съответствието, или използва дъщерните си дружества, той гарантира, че подизпълнителят или дъщерното дружество отговаря на изискванията, предвидени в член 31, и информира нотифициращия орган за това.
2. Нотифицираните органи поемат пълната отговорност за задачите, изпълнявани от подизпълнители или дъщерни дружества.
3. Дейностите могат да бъдат възлагани на подизпълнители или изпълнявани от дъщерни дружества само със съгласието на доставчика. Нотифицираните органи оповестяват публично списък на своите дъщерни дружества.
4. Съответните документи относно оценката на квалификацията на подизпълнителя или на поделението и работата, извършена от тях съгласно настоящия регламент, се съхраняват на разположение на нотифициращия орган за срок от пет години от датата на прекратяване на възлагането.

Член 34

Задължения на нотифицираните органи при осъществяване на дейността им

1. Нотифицираните органи проверяват съответствието на високорисковите системи с ИИ съгласно процедурите за оценяване на съответствието, установени в член 43.
2. При изпълнението на своите дейности нотифицираните органи избягват ненужната тежест за доставчиците и надлежно вземат предвид размера на доставчика, сектора му на дейност, неговата структура и степента на сложност на съответната високорискова система с ИИ, по-специално с оглед на свеждането до минимум на административната тежест и разходите за привеждане в съответствие за микро- и малките предприятия по смисъла на Препоръка 2003/361/ЕО. Нотифицираният орган зачита степента на възискателност и равнището на защита, необходими за осигуряване на съответствието на високорисковата система с ИИ с изискванията на настоящия регламент.
3. Нотифицираните органи съхраняват на разположение на нотифициращия орган, посочен в член 28, и при поискване му предоставят цялата необходима документация, включително документацията на доставчика, за да осигурят на този орган възможност да извършва дейностите си по оценяване, определяне, нотифициране и мониторинг и да улеснят оценяването, описано в настоящия раздел.

Член 35

Идентификационни номера и списъци на нотифицираните органи

1. Комисията определя единен идентификационен номер на всеки нотифициран орган, дори когато даден орган е нотифициран съгласно повече от един акт на Съюза.
2. Комисията оповестява публично списъка на нотифицираните съгласно настоящия регламент органи, включително идентификационните им номера и дейностите, за които те са били нотифицирани. Комисията поддържа този списък актуален.

Член 36

Промени в нотификациите

1. Нотифицираният орган нотифицира Комисията и другите държави членки за всички съответни промени в нотификацията на нотифициран орган чрез инструмента за електронно нотифициране, посочен в член 30, параграф 2.
2. Процедурите, установени в членове 29 и 30, се прилагат по отношение на разширяването на обхвата на нотификацията.

За промени в нотификацията, различни от разширяването на нейния обхват, се прилагат процедурите, предвидени в параграфи 3-9.

3. Когато даден нотифициран орган реши да прекрати дейностите си по оценяване на съответствието, той уведомява нотифициращия орган и съответните доставчици във възможно най-кратък срок, а в случай на планирано прекратяване — най-малко една година преди да прекрати дейността си. Сертификатите на нотифицирания орган може да запазят валидността си за срок от девет месеца след прекратяване на дейността на нотифицирания орган, при условие че друг нотифициран орган писмено е потвърдил, че ще поеме отговорност за високорисковите системи с ИИ, обхванати от тези сертификати. Вторият нотифициран орган извършва пълно оценяване на високорисковите системи с ИИ, засегнати от изтичането на този деветмесечен срок, преди да издаде нови сертификати за тези системи. Когато нотифицираният орган прекрати дейността си, нотифициращият орган оттегля определянето.

4. Когато нотифициращ орган има достатъчно основания да счита, че нотифициран орган вече не отговаря на изискванията, предвидени в член 31, или че не изпълнява задълженията си, нотифициращият орган незабавно проучва въпроса възможно най-задълбочено. Във връзка с това 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 вече не отговаря на изискванията, предвидени в член 31, или че не изпълнява задълженията си, нотифициращият орган ограничава обхвата, спира действието или оттегля определянето според случая, в зависимост от това колко съществени са пропуските при неизпълнението на тези изисквания или на тези задължения. Той незабавно информира за това Комисията и другите държави членки.

5. Когато действието на определянето му е било спряно или определянето му е било ограничено или изцяло или частично оттеглено, нотифицираният орган уведомява засегнатите доставчици в рамките на 10 дни.

6. В случай на ограничаване, спиране на действието или оттегляне на определянето нотифициращият орган предприема подходящи мерки, за да гарантира, че досиетата на съответния нотифициран орган се съхраняват, и предоставя тези досиета на нотифициращите органи в други държави членки и на органите за надзор на пазара при поискване от тяхна страна.

7. В случай на ограничаване, спиране на действието или оттегляне на определянето нотифициращият орган:

- а) оценява въздействието върху сертификатите, издадени от нотифицирания орган;
 - б) представя доклад с констатациите си на Комисията и другите държави членки в срок от три месеца след като е уведомил за промените в определянето;
 - в) изисква от нотифицирания орган да спре действието или да отнеме в рамките на разумен, определен от органа срок всички сертификати, които са издадени неоснователно, за да се осигури непрекъснато съответствие на високорисковите системи с ИИ, намиращи се на пазара;
 - г) информира Комисията и държавите членки за сертификатите, чието спиране или отнемане е изискал;
 - д) предоставя на националните компетентни органи на държавата членка, в която се намира регистрираното място на стопанска дейност на доставчика, цялата необходима информация за сертификатите, за които е поискал спиране на действието или отнемане; когато е необходимо, този орган предприема подходящи мерки, за да се избегне евентуален риск за здравето, безопасността или основните права.
8. С изключение на неоснователно издадените сертификати и в случаите, когато е било спряно действието на определянето или то е било ограничено, сертификатите остават валидни при някои от следните обстоятелства:
- а) когато нотифициращият орган е потвърдил в срок от един месец от спирането на действието или ограничаването, че не съществува риск за здравето, безопасността или основните права по отношение на сертификатите, засегнати от спирането на действието или ограничаването, и когато нотифициращият орган е определил график и действия, които да доведат до отмяна на спирането на действието или ограничаването; или
 - б) когато нотифициращият орган е потвърдил, че няма да се издават, изменят или преиздават сертификати, свързани със спирането на действието, докато трае това спиране на действието или ограничаване, и е посочил дали нотифицираният орган е способен да продължи да наблюдава и да носи отговорност за съществуващите сертификати, издадени за срока на спирането на действието или ограничаването; в случай че нотифициращият орган определи, че нотифицираният орган не е способен да поддържа съществуващи издадени сертификати, в срок от три месеца от спирането на действието или ограничаването доставчикът на системата, обхваната от сертификата, потвърждава писмено на националните компетентни органи на държавата членка, в която се намира регистрираното му място на стопанска дейност, че друг квалифициран нотифициран орган временно поема функциите на нотифицирания орган, за да наблюдава и да продължи да носи отговорност за сертификатите за срока на спиране на действието или ограничаването.

9. С изключение на неоснователно издадените сертификати и в случаите, когато определянето е било оттеглено, сертификатите запазват валидността си за срок от девет месеца при следните обстоятелства:

- а) националният компетентен орган на държавата членка, в която се намира регистрираното място на стопанска дейност на доставчика на високорисковата система с ИИ, обхваната от сертификата, е потвърдил, че не съществува риск за здравето, безопасността или основните права, свързан със съответните високорискови системи с ИИ; и
- б) друг нотифициран орган писмено е потвърдил, че ще поеме непосредствената отговорност за тези системи с ИИ и ще приключи оценяването им в рамките на 12 месеца, считано от оттеглянето на определянето.

При условията, посочени в първа алинея, националният компетентен орган на държавата членка, в която е регистрирано мястото на стопанска дейност на доставчика на системата, обхваната от сертификата, може да удължи срока на временната валидност на сертификатите за допълнителни срокове от три месеца, които общо не надхвърлят 12 месеца.

Националният компетентен орган или нотифицираният орган, поемащ функциите на нотифицирания орган, засегнат от промяната в определянето, незабавно информира за това Комисията, останалите държави членки и другите нотифицирани органи.

Член 37

Оспорване на компетентността на нотифицираните органи

1. Когато е необходимо, Комисията проучва всички случаи, при които има основания за съмнение в компетентността на даден нотифициран орган или в това дали нотифицираният орган продължава да изпълнява изискванията, предвидени в член 31, и произтичащите от тях отговорности.
2. Нотифициращият орган предоставя на Комисията, при искане от нейна страна, всяка информация, имаща отношение към нотификацията или поддържането на компетентността на съответния нотифициран орган.
3. Комисията гарантира, че цялата чувствителна информация, получена в хода на проучването съгласно настоящия член, се третира като поверителна в съответствие с член 78.
4. Когато Комисията констатира, че нотифициран орган не отговаря или вече не отговаря на изискванията за нотифицирането му, тя информира нотифициращата държава членка за това и изисква от нея да предприеме необходимите коригиращи мерки, включително, ако е необходимо, спиране на действието или оттегляне на нотификацията. Когато държавата членка не предприеме необходимите коригиращи мерки, Комисията може чрез акт за изпълнение да спре действието, да ограничи или да оттегли определянето. Този акт за изпълнение се приема в съответствие с процедурата по разглеждане, посочена в член 98, параграф 2.

Член 38

Координация на нотифицираните органи

1. Комисията гарантира, че по отношение на високорисковите системи с ИИ между нотифицираните органи, работещи по процедури за оценяване на съответствието съгласно настоящия регламент, се установяват подходяща координация и сътрудничество, които се осъществяват по адекватен начин под формата на секторна група от нотифицирани органи.
2. Всеки нотифициращ орган гарантира, че нотифицираните от него органи участват в работата на групата, посочена в параграф 1, пряко или чрез определени представители.
3. Комисията осигурява обмена на знания и най-добри практики между нотифициращите органи.

Член 39

Органи за оценяване на съответствието от трети държави

На органите за оценяване на съответствието, създадени съгласно правото на трета държава, с която Съюзът е сключил споразумение, могат да бъде разрешено да извършват дейностите на нотифицираните органи съгласно настоящия регламент, при условие че отговарят на изискванията, предвидени в член 31, или че гарантират равностойно равнище на съответствие.

РАЗДЕЛ 5

Стандарти, оценяване на съответствието, сертификати и регистрация

Член 40

Хармонизирани стандарти и стандартизационни документи

1. Високорисковите системи с ИИ, които са в съответствие с хармонизираните стандарти или на части от тях, справочната информация за които е била публикувана в *Официален вестник на Европейския съюз* в съответствие с Регламент (ЕС) № 1025/2012, се считат за съответстващи на изискванията, установени в раздел 2 от настоящата глава, или, в зависимост от случая, на задълженията, установени в глава V, раздели 2 и 3 от настоящия регламент, доколкото тези стандарти обхващат посочените изисквания или задължения.

2. В съответствие с член 10 от Регламент (ЕС) № 1025/2012 Комисията отправя без ненужно забавяне искания за стандартизация, обхващащи всички изисквания, установени в раздел 2 от настоящата глава, и доколкото е приложимо, искания за стандартизация, обхващащи задълженията, установени в глава V, раздели 2 и 3 от настоящия регламент. В искането за стандартизация се изискват и документи относно процесите на докладване и документиране с цел подобряване на ресурсната ефективност на системите с ИИ, като например намаляване на потреблението на енергия и други ресурси на високорисковата система с ИИ по време на жизнения ѝ цикъл, както и относно ефективното от енергийна гледна точка разработване на модели на ИИ с общо предназначение. При изготвянето на искане за стандартизация Комисията се консултира със Съвета по ИИ и съответните заинтересовани страни, включително консултативния форум.

Когато отправя искане за стандартизация до европейските организации по стандартизация, Комисията посочва, че стандартите трябва да бъдат ясни, съгласувани, включително със стандартите, разработени в различните сектори за продукти, обхванати от съществуващото законодателство на Съюза за хармонизация, посочено в приложение I, и да имат за цел да се гарантира, че високорисковите системи с ИИ или моделите на ИИ с общо приложение, пуснати на пазара или пуснати в действие в Съюза, изпълняват съответните изисквания или задължения, установени в настоящия регламент.

Комисията изисква от европейските организации за стандартизация да представят доказателства за положените от тях максимални усилия за постигане на целите, посочени в първа и втора алинея от настоящия параграф, в съответствие с член 24 от Регламент (ЕС) № 1025/2012.

3. Участниците в процеса на стандартизация се стремят да насърчават инвестициите и иновациите в областта на ИИ, включително чрез повишаване на правната сигурност, както и конкурентоспособността и растежа на пазара на Съюза, да допринасят за укрепването на глобалното сътрудничество в областта на стандартизацията и отчитането на съществуващите международни стандарти в областта на ИИ, които са в съответствие с ценностите, основните права и интереси на Съюза, и да подобряват управлението с участието на множество заинтересовани страни, като осигуряват ефективно участие на всички заинтересовани страни в съответствие с членове 5, 6 и 7 от Регламент (ЕС) № 1025/2012

Член 41

Общи спецификации

1. Комисията може да приема актове за изпълнение за установяване на общи спецификации за изискванията, установени в раздел 2 от настоящата глава, или, доколкото е приложимо, за задълженията, установени в глава V, раздели 2 и 3, когато са изпълнени следните условия:

а) съгласно член 10, параграф 1 от Регламент (ЕС) № 1025/2012 Комисията е поискала от една или повече европейски организации за стандартизация да изготвят хармонизиран стандарт за изискванията, установени в раздел 2 от настоящата глава, или, доколкото е приложимо, за задълженията, установени в глава V, раздели 2 и 3, и:

и) искането не е прието от нито една от европейските организации за стандартизация; или

- ii) хармонизираните стандарти, изготвени в резултат на това искане, не са представени в срока, определен в съответствие с член 10, параграф 1 от Регламент (ЕС) № 1025/2012; или
 - iii) съответните хармонизирани стандарти не предлагат в достатъчна степен решение във връзка с опасенията, свързани с основните права; или
 - iv) хармонизираните стандарти не са в съответствие с искането; и
- б) в *Официален вестник на Европейския съюз* не е публикувана справочна информация за хармонизирани стандарти, обхващащи посочените в раздел 2 от настоящата глава изисквания или, в зависимост от случая, задълженията, установени в глава V, раздели 2 и 3, в съответствие с Регламент (ЕС) № 1025/2012 и не се очаква да бъдат публикувани такива данни в разумен срок.

При изготвянето на общите спецификации Комисията се консултира с консултативния форум, посочен в член 67.

Актовете за изпълнение, посочени в първа алинея от настоящия параграф, се приемат в съответствие с процедурата по разглеждане, посочена в член 98, параграф 2.

2. Преди да изготви проект за акт за изпълнение, Комисията информира комитета, посочен в член 22 от Регламент (ЕС) № 1025/2012, че счита за изпълнени условията, предвидени в параграф 1 от настоящия член.

3. Високорисковите системи с ИИ или модели на ИИ с общо предназначение, които са в съответствие с общите спецификации, посочени в параграф 1, или на части от тези спецификации, се считат за съответстващи на изискванията, установени в раздел 2 от настоящата глава, или, в зависимост от случая, на задълженията, установени в глава V, раздели 2 и 3, доколкото тези общи спецификации обхващат посочените изисквания или задължения.

4. Когато хармонизиран стандарт е приет от европейска организация за стандартизация и на Комисията е предложено да публикува справочната информация за този стандарт в *Официален вестник на Европейския съюз*, Комисията оценява хармонизирания стандарт в съответствие с Регламент (ЕС) № 1025/2012. Когато в *Официален вестник на Европейския съюз* се публикува справочната информация за хармонизиран стандарт, Комисията отменя актовете за изпълнение, посочени в параграф 1, или части от тях, които обхващат същите изисквания, установени в раздел 2 от настоящата глава, или, в зависимост от случая, същите задължения, установени в глава V, раздели 2 и 3.

5. Когато доставчиците на високорискови системи с ИИ или модели на ИИ с общо предназначение не спазват общите спецификации, посочени в параграф 1, те надлежно доказват, че са приели технически решения, които отговарят на изискванията, посочени в раздел 2 от настоящата глава, или, в зависимост от случая, задълженията, установени в глава V, раздели 2 и 3, до равнище, което е най-малко равностойно на тях.

6. Когато държава членка счита, че дадена обща спецификация не отговаря напълно на изискванията, установени в раздел 2 от настоящата глава, или, в зависимост от случая, задълженията, установени в глава V, раздели 2 и 3, тя информира Комисията за това, като прилага подробно обяснение. Комисията прави оценка на тази информация и ако е целесъобразно, изменя акта за изпълнение за установяване на съответната обща спецификация.

Член 42

Презумпция за съответствие с определени изисквания

1. Високорисковите системи с ИИ, които са били обучени и изпитани въз основа на данни, отразяващи конкретната географска, контекстуална, поведенческа или функционална среда, в която е предназначено да бъдат използвани, се считат за съответстващи на приложимите изисквания, предвидени в член 10, параграф 4.

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 и справочната информация за които е била публикувана в *Официален вестник на Европейския съюз*, се считат за съответстващи на изискванията за киберсигурност, установени 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, посочени в точка 1 от приложение III, когато при доказване на съответствието на високорискова система с ИИ с изискванията, установени в раздел 2, доставчикът е приложил хармонизираните стандарти, посочени в член 40, или, когато е приложимо, общите спецификации, посочени в член 41, доставчикът избира една от посочените по-долу процедури за оценяване на съответствието, основани на:

- а) вътрешния контрол, посочен в приложение VI; или
- б) оценяването на системата за управление на качеството и оценяване на техническата документация с участието на нотифициран орган, посочена в приложение VII.

При доказването на съответствието на високорискова система с ИИ с изискванията, установени в раздел 2, доставчикът прилага процедурата за оценяване на съответствието, посочена в приложение VII, когато:

- а) не съществуват хармонизираните стандарти, посочени в член 40, и не са налице общите спецификации, посочени в член 41;
- б) доставчикът не е приложил или е приложил само част от хармонизирания стандарт;
- в) общите спецификации, посочени в буква а), съществуват, но доставчикът не ги е приложил;
- г) един или повече от хармонизираните стандарти, посочени в буква а), са публикувани с ограничение - само по отношение на частта от стандарта, която е била ограничена.

За целите на процедурата за оценяване на съответствието, посочена в приложение VII, доставчикът може да избере всеки от нотифицираните органи. Когато обаче високорисковата система с ИИ е предназначена за пускане в действие от правоохранителни органи, имиграционни органи или органи в областта на убежището или от институции, органи, служби или агенции на Съюза, органът за надзор на пазара, посочен в член 74, параграф 8 или 9, в зависимост от 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.

3. За високорисковите системи с ИИ, обхванати от законодателството на Съюза за хармонизация, посочено в раздел А от приложение I, доставчикът следва съответната процедура за оценяване на съответствието, изисквана съгласно посочените правни актове. Изискванията, установени в раздел 2 от настоящата глава дял, се прилагат за тези високорискови системи с ИИ и са част от това оценяване. Прилагат се също така 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 посочените правни актове, имат право да упражняват контрол за съответствието на високорисковите системи с ИИ с изискванията, установени в раздел 2, при условие че съответствието на тези нотифицирани органи с изискванията, предвидени в член 31, параграфи 4, 5, 10 и 11, е било оценено в контекста на процедурата по нотифициране съгласно посочените правни актове.

Когато правен акт, посочен в раздел А от приложение I, дава възможност на производителя на продукта да се откаже от оценяване на съответствието от трето лице, при условие че е приложил всички хармонизирани стандарти, обхващащи всички съответни изисквания, производителят може да използва тази възможност само ако е приложил също така хармонизираните стандарти или, когато е приложимо, общите спецификации, посочени в член 41, обхващащи всички изисквания, установени в раздел 2 от настоящата глава.

4. Високорисковите системи с ИИ, които вече са преминали процедура за оценяване на съответствието, преминават нова процедура за оценяване на съответствието в случай на съществено изменение, независимо дали изменената система е предназначена за по-нататъшно разпространение или продължава да се използва от настоящия внедрител.

За високорисковите системи с ИИ, които продължават да се обучават след пускането им на пазара или пускането им в действие, не представляват съществено изменение 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.

5. На Комисията се предоставя правомощието да приема делегирани актове в съответствие с член 97 за изменение на приложения VI и VII с цел актуализирането им с оглед на техническия напредък.

6. На Комисията се предоставя правомощието са приема делегирани актове в съответствие с член 97 с цел изменение на параграфи 1 и 2 от настоящия член 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 тези 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, издавани от нотифицирани органи в съответствие с приложение VII, се изготвят на език, който лесно може да бъде разбран от съответните органи в държавата членка, в която е установен нотифицираният орган.

2. Сертификатите са валидни за посочения в тях срок, който не надвишава пет години за системите с ИИ, обхванати от приложение I, и четири години за системите с ИИ, обхванати от приложение III. По искане на доставчика валидността на сертификата може да се удължи за допълнителни срокове, всеки от които не надхвърля пет години за системи с ИИ, обхванати от приложение I, и четири години за системи с ИИ, обхванати от приложение III, въз основа на последващо оценяване съгласно приложимите процедури за оценяване на съответствието. Всяко допълнение към сертификата остава валидно, при условие че съответният сертификат е валиден.

3. Когато нотифициран орган установи, че система с ИИ вече не отговаря на изискванията, установени в раздел 2, 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.

Трябва да съществува процедура за обжалване на решенията на нотифицираните органи, включително за издадени сертификати за съответствие.

Член 45

Задължения на нотифицираните органи за информиране

1. Нотифицираните органи информират нотифицирания орган за следното:

- а) всички сертификати на Съюза за оценяване на техническата документация, всички допълнения към тези сертификати и всички одобрения на системи за управление на качеството, издадени в съответствие с изискванията на приложение VII;
- б) всеки отказ за издаване, ограничаване, спиране на действието или отнемане на сертификат на Съюза за оценяване 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 дейности и 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 Съюза за оценяване на техническата документация или допълнения към тях, които е отказал, отнел, спрял е действието им или по друг начин е ограничил, и при поискване — за издадените сертификати и/или допълнения към тях.

3. Всеки нотифициран орган предоставя на другите нотифицирани органи, осъществяващи подобни дейности по оценяване на съответствието, чийто предмет са същите видове системи с ИИ, съответната информация по въпроси, свързани с отрицателни и, при поискване, положителни резултати от оценяването на съответствието.
4. Нотифициращите органи гарантират поверителността на информацията, която получават в съответствие с член 78.

Член 46

Дерогация от процедурата за оценяване на съответствието

1. Чрез дерогация от член 43 и при надлежно обосновано искане всеки орган за надзор на пазара може да разреши пускането на пазара или пускането в действие на конкретни високорискови системи с ИИ на територията на съответната държава членка по извънредни причини, свързани с обществената сигурност или защитата на живота и здравето на хората, опазването на околната среда или защитата на ключови промишлени и инфраструктурни активи. Това разрешение се издава за ограничен срок, докато се провеждат необходимите процедури за оценяване на съответствието, като се вземат предвид извънредните причини, обосноваващи дерогацията. Тези процедури се провеждат без ненужно забавяне.
2. В надлежно обосновани спешни случаи по извънредни причини, свързани с обществената сигурност, или при конкретна, съществена и непосредствена заплаха за живота или физическата безопасност на физически лица, правоохранителните органи или органите за гражданска защита могат да пуснат в действие конкретна високорискова система с ИИ без разрешението, посочено в параграф 1, при условие че това разрешение бъде поискано без ненужно забавяне по време на използването или след него. Ако разрешението, посочено в параграф 1, бъде отказано, използването на високорисковата система с ИИ се прекратява незабавно и всички резултати и крайни продукти от това използване незабавно се премахват.
3. Разрешението, посочено в параграф 1, се издава само ако органът за надзор на пазара заключи, че високорисковата система с ИИ съответства на изискванията, установени в раздел 2. Органът за надзор на пазара информира Комисията и другите държави членки за всяко разрешение, издадено съгласно параграфи 1 и 2. Това задължение не обхваща чувствителни оперативни данни във връзка с дейностите на правоохранителните органи.
4. Когато в рамките на 15 календарни дни от получаването на информацията, посочена в параграф 3, не е повдигнато възражение от държава членка или 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.
5. Когато в срок от 15 календарни дни от получаването на информацията, посочена в параграф 3, 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 3, е необосновано, Комисията без забавяне започва консултации със съответната държава членка. Провеждат се консултации със съответните оператори и им се предоставя възможност да представят своето мнение. Комисията решава дали разрешението е обосновано, като взема предвид тези консултации. Комисията съобщава решението си на съответната държава членка и съответните оператори.
6. Ако Комисията прецени, че разрешението не е обосновано, органът за надзор на пазара на съответната държава членка го отнема.
7. За високорисковите системи с ИИ, свързани с продукти, обхванати от законодателството на Съюза за хармонизация, посочено в раздел А от приложение I, се прилагат само дерогациите от оценката на съответствието, установени в посоченото законодателство на Съюза за хармонизация.

Член 47

ЕС декларация за съответствие

1. Доставчикът изготвя писмена машинночетима, печатна или електронно подписана декларация на ЕС за съответствие за всяка високорискова система с ИИ и я съхранява на разположение на националните компетентни органи в продължение на 10 години след пускането на пазара или пускането в действие на високорисковата система с ИИ. В ЕС декларацията за съответствие се посочва високорисковата система с ИИ, за която тя е изготвена. При поискване, на съответния национален компетентен орган се представя копие от ЕС декларацията за съответствие.

2. В ЕС декларацията за съответствие се посочва, че високорисковата система с ИИ отговаря на изискванията, установени в раздел 2. ЕС декларацията за съответствие съдържа информацията, посочена в приложение V, и се превежда на език, който може лесно да бъде разбран от националните компетентни органи на държавите членки, в които се пуска на пазара или се предоставя високорисковата система с ИИ.
3. Когато високорисковите системи с ИИ се уреждат от друго законодателство на Съюза за хармонизация, което също изисква ЕС декларация за съответствие, се изготвя единна ЕС декларация за съответствие по отношение на всички правни актове на Съюза, приложими към високорисковата система с ИИ. Декларацията съдържа цялата информация, необходима за установяване на законодателството на Съюза за хармонизация, с който е свързана съответната декларация.
4. Като изготвя ЕС декларацията за съответствие, доставчикът поема отговорността за съответствието с изискванията, установени в раздел 2. Доставчикът актуализира ЕС декларацията за съответствие, когато това е целесъобразно.
5. Комисията приема делегирани актове в съответствие с член 97 за изменение на приложение V с цел актуализиране на съдържанието на ЕС декларацията за съответствие, съдържаща се в приложение V, за да се въведат елементи, които са станали необходими с оглед на техническия напредък.

Член 48

Маркировка „СЕ“

1. За маркировката „СЕ“ се прилагат общите принципи, установени в член 30 от Регламент (ЕО) № 765/2008.
2. За високорискови системи с ИИ, които са само цифрови, се използва цифрова маркировка „СЕ“ само ако тя е лесно достъпна чрез интерфейса, от който се осъществява достъпът до тази система, или чрез лесно достъпен машинночетим код или друго електронно средство.
3. 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, маркировката се нанася върху опаковката или в придружаващите документи, в зависимост от случая.
4. 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 на нотифицирания орган се нанася от самия орган или, въз основа на неговите указания, от доставчика или от негов упълномощен представител. Идентификационният номер се посочва също така върху всеки рекламен материал, който указва, че високорисковата система с ИИ отговаря на изискванията за маркировката „СЕ“.
5. Когато към високорисковите системи с ИИ се прилага друг правен акт на Съюза, който също предвижда нанасяне на маркировката „СЕ“, маркировката „СЕ“ указва, че високорисковата система с ИИ отговаря и на изискванията на това друг правен акт.

Член 49

Регистрация

1. Преди пускането на пазара или пускането в действие на високорискова система с ИИ, посочена в приложение III, с изключение на високорисковите системи с ИИ, посочени в точка 2 от приложение III, доставчикът или, когато е приложимо, упълномощеният представител регистрира себе си и своята система в базата данни на ЕС, посочена в член 71.
2. Преди пускането на пазара или пускането в действие на система с ИИ, за която доставчикът е стигнал до заключението, че не е високорискова съгласно член 6, параграф 3, този доставчик или, когато е приложимо, упълномощеният представител регистрира себе си и тази система в базата данни на ЕС, посочена в член 71.
3. Преди пускането в действие или използването на високорискова система с ИИ, посочена в приложение III, с изключение на високорисковите системи с ИИ, посочени в точка 2 от приложение III, внедрителите, които са публични органи или институции, органи, служби или агенции на Съюза, или лица, действащи от тяхно име, се регистрират, избират системата и регистрират използването ѝ в базата данни на ЕС, посочена в член 71.

4. За високорисковите системи с ИИ, посочени в точки 1, 6 и 7 от приложение III в правоохранителната област или в областта на миграцията, убежището и управлението на граничния контрол, регистрацията, посочена в параграфи 1, 2 и 3 от настоящия член, се извършва в защитен непубличен раздел от базата данни на ЕС, посочена в член 71, и включва, в зависимост от случая, само посочената по-долу информация съгласно:

- а) раздел А, точки 1 – 10 от приложение VIII, с изключение на точки 6, 8 и 9;
- б) раздел Б, точки 1 – 5 и точки 8 и 9 от приложение VIII;
- в) раздел В, точки 1 – 3 от приложение VIII;
- г) точки 1, 2, 3 и 5 от приложение IX.

Само Комисията и националните органи, посочени в член 74, параграф 8, имат достъп до съответните раздели с ограничен достъп от базата данни на ЕС, изброени в първа алинея от настоящия член.

5. Високорисковите системи с ИИ, посочени в точка 2 от приложение III, се регистрират на национално равнище.

ГЛАВА IV

ЗАДЪЛЖЕНИЯ ЗА ПРОЗРАЧНОСТ ЗА ДОСТАВЧИЦИТЕ И ВНЕДРИТЕЛИТЕ НА ОПРЕДЕЛЕНИ СИСТЕМИ С ИИ

Член 50

Задължения за прозрачност за доставчиците и внедрителите на определени системи с ИИ

1. Доставчиците гарантират, че системите с ИИ, предназначени да взаимодействат пряко с физически лица, са проектирани и разработени по такъв начин, че съответните физически лица да бъдат информирани, че взаимодействат със система с ИИ, освен ако това не е очевидно от гледна точка на физическо лице, което е в разумни граници осведомено, наблюдателно и съобразително предвид обстоятелствата и контекстът на използване. Това задължение не се прилага за системи с ИИ, разрешени по закон за разкриване, предотвратяване, разследване или наказателно преследване на престъпления, при спазване на подходящи гаранции за правата и свободите на трети лица, освен когато тези системи са общодостъпни с цел подаване на сигнали за престъпление.

2. Доставчиците на системи с ИИ, включително системи с ИИ с общо предназначение, които генерират синтетично аудио съдържание, изображения, видео или текстово съдържание, гарантират, че резултатите от системата с ИИ са представени в машинночитим формат и са разпознаваеми като изкуствено генерирани или обработени. Доставчиците гарантират, че техните технически решения са ефективни, оперативно съвместими, сигурни и надеждни, доколкото това е технически осъществимо, като се вземат предвид особеностите и ограниченията на различните видове съдържание, разходите за прилагане и общопризнатите съвременни технически постижения, които може да бъдат отразени в подходящи технически стандарти. Това задължение не се прилага, доколкото системите с ИИ изпълняват помощна функция при стандартно редактиране или не променят съществено въведените от внедрителя входящи данни или семантиката им, или когато са разрешени по закон за разкриване, предотвратяване, разследване или наказателно преследване на престъпления.

3. Внедрителите на системи за разпознаване на емоции или на системи за биометрично категоризиране информират физическите лица, които са изложени на съответната система, за функционирането на системата и обработват личните данни в съответствие с регламенти (ЕС) 2016/679 и (ЕС) 2018/1725 и Директива (ЕС) 2016/680, в зависимост от случая. Това задължение не се прилага за системи с ИИ, използвани за биометрично категоризиране и разпознаване на емоции, които са разрешени по закон за разкриване, предотвратяване, разследване на престъпления, при спазване на подходящи гаранции за правата и свободите на трети лица и в съответствие с правото на Съюза.

4. Внедрителите на система с ИИ за генериране или обработка на изображения, аудио или видео съдържание, които представляват убедителен фалшификат, оповестяват обстоятелството, че съдържанието е изкуствено генерирано или обработено. Това задължение не се прилага, когато използването е разрешено по закон за разкриване, предотвратяване, разследване или наказателно преследване на престъпления. Когато съдържанието е част от произведение или програма, които имат очевиден творчески, сатиричен, артистичен, художествен или подобен характер, задълженията за прозрачност, посочени в настоящия параграф, се ограничават до оповестяване на съществуването на такова генерирано или обработено съдържание по подходящ, ясен и видим начин, който не възпрепятства показването или използването на произведението.

Внедрителите на система с ИИ, която генерира или обработва текст, публикуван с цел информиране на обществеността по въпроси от обществен интерес, оповестяват обстоятелството, че текстът е бил изкуствено генериран или обработен. Това задължение не се прилага, когато използването е разрешено по закон за разкриване, предотвратяване, разследване или наказателно преследване на престъпления или когато генерираното от ИИ съдържание е преминало през процес на преглед от човек или редакционен контрол и когато физическо или юридическо лице носи редакционна отговорност за публикуването на съдържанието.

5. Информацията, посочена в параграфи 1 – 4, се предоставя на засегнатите физически лица по ясен и добре различим начин най-късно в момента на първото взаимодействие или първия контакт. Информацията трябва да отговаря на приложимите изисквания за достъпност.

6. Параграфи 1 – 4 не засягат изискванията и задълженията, установени в глава III, нито други задължения за прозрачност, установени в правото на Съюза или в националното право спрямо внедрителите на системи с ИИ.

7. Службата по ИИ насърчава и улеснява изготвянето на кодекси за поведение на равнището на Съюза, за да се улесни ефективното изпълнение на задълженията по отношение на откриването и обозначаването на изкуствено генерирано или обработено съдържание. Комисията може да приема актове за изпълнение за одобряване на тези кодекси за добри практики в съответствие с процедурата, предвидена в член 56, параграф 6. Когато счете кодекса за неподходящ, Комисията може да приеме акт за изпълнение, в който се установяват общите правила за изпълнението на тези задължения в съответствие с процедурата по разглеждане, предвидена в член 98, параграф 2.

ГЛАВА V

МОДЕЛИ НА ИИ С ОБЩО ПРЕДНАЗНАЧЕНИЕ

РАЗДЕЛ 1

Правила за класификация

Член 51

Класификация на моделите на ИИ с общо предназначение като модели на ИИ с общо предназначение, пораждащи системен риск

1. Модел на ИИ с общо предназначение се класифицира като модел на ИИ с общо предназначение, пораждащ системен риск, ако отговаря на някое от посочените по-долу условия:

- а) има способности с висока степен на въздействие, оценени въз основа на подходящи технически инструменти и методологии, включително показатели и сравнителни показатели;
- б) въз основа на решение на Комисията, по собствена инициатива или след приоритетен сигнал от експертната група, има способности или въздействие, равностойни на посочените в буква а), като се вземат предвид критериите, посочени в приложение XIII.

2. Счита се, че даден модел на ИИ с общо предназначение има способности с висока степен на въздействие съгласно параграф 1, буква а), когато общото количество изчисления, използвани за неговото обучение, измерено при операции с плаваща запетая, е по-голямо от 10^{25} .

3. Комисията приема делегирани актове в съответствие с член 97 за изменение на праговете, посочени в параграфи 1 и 2 от настоящия член, както и за допълване на референтните стойности и показателите с оглед на технологичното развитие, като например алгоритмични подобрения или повишена ефективност на хардуера, когато е необходимо, за да могат тези прагове да отразяват съвременните постижения.

Член 52

Процедура

1. Когато модел на ИИ с общо предназначение отговаря на условието, посочено в член 51, параграф 1, буква а), съответният доставчик уведомява Комисията без забавяне и при всички случаи в срок от две седмици след като това изискване е изпълнено или стане известно, че ще бъде изпълнено. Това уведомление включва необходимата информация, за да се докаже, че съответното изискване е изпълнено. Ако Комисията получи информация за модел на ИИ с общо предназначение, пораждащ системни рискове, за които не е била уведомена, тя може да реши да го определи като модел, пораждащ системен риск.

2. Доставчикът на модел на ИИ с общо предназначение, който отговаря на условието, посочено в член 51, параграф 1, буква а), може да представи заедно със своето уведомление достатъчно обосновани аргументи, за да докаже, че по изключение, въпреки че отговаря на това изискване, моделът на ИИ с общо предназначение не поражда, поради специфичните си характеристики, системни рискове и поради това не следва да бъде класифициран като модел на ИИ с общо предназначение, пораждащ системен риск.

3. Когато Комисията стигне до заключението, че аргументите, представени съгласно параграф 2, не са достатъчно обосновани и съответният доставчик не е бил в състояние да докаже, че моделът на ИИ с общо предназначение не поражда системни рискове поради специфичните си характеристики, тя отхвърля тези аргументи и моделът на ИИ с общо предназначение се счита за модел на ИИ с общо предназначение, пораждащ системен риск.

4. Комисията може въз основа на критериите, посочени в приложение XIII, да определи модел на ИИ с общо предназначение като пораждащ системни рискове, по собствена инициатива или след приоритетен сигнал от експертната група съгласно член 90, параграф 1, буква а).

На Комисията се предоставя правомощието да приема делегирани актове в съответствие с член 97 с цел изменение на приложение XIII чрез конкретизиране и актуализиране на критериите, посочени в приложението.

5. При обосновано искане от доставчик, чийто модел е определен като модел на ИИ с общо предназначение, пораждащ системен риск, съгласно параграф 4, Комисията взема предвид искането и може да реши да направи повторна оценка дали все още може да се счита, че моделът на ИИ с общо предназначение поражда системни рискове въз основа на критериите, установени в приложение XIII. Това искане следва да съдържа обективни, подробни и нови причини, възникнали след решението за определяне. Доставчиците могат да поискат повторна оценка най-рано шест месеца след решението за определяне. Ако след повторната оценка Комисията реши да продължи да счита модела за модел на ИИ с общо предназначение, пораждащ системен риск, доставчиците могат да поискат нова повторна оценка най-рано шест месеца след това решение.

6. Комисията осигурява публикуването на списък на моделите на ИИ с общо предназначение, пораждащи системен риск, и актуализира този списък, без да се засяга необходимостта от закрила и защита на правата върху интелектуалната собственост и поверителната търговска информация или търговските тайни в съответствие с правото на Съюза и националното право.

РАЗДЕЛ 2

Задължения на доставчиците на модели на ИИ с общо предназначение

Член 53

Задължения на доставчиците на модели на ИИ с общо предназначение

1. Доставчиците на модели на ИИ с общо предназначение:

- а) изготвят и актуализират техническата документация на модела, включително процеса на неговото обучение и изпитване, както и резултатите от неговата оценка, която съдържа най-малко информацията, посочена в приложение XI, с цел тя да бъде предоставена при поискване на Службата по ИИ и на националните компетентни органи;
- б) изготвят, актуализират и предоставят информация и документация на доставчиците на системи с ИИ, които възнамеряват да интегрират модела на ИИ с общо предназначение в своите системи с ИИ. Без да се засяга необходимостта от закрила и защита на правата върху интелектуалната собственост и поверителната търговска информация или търговските тайни в съответствие с правото на Съюза и националното право, информацията и документацията:
 - i) дават възможност на доставчиците на системи с ИИ да разберат добре способностите и ограниченията на модела на ИИ с общо предназначение и да изпълняват задълженията си съгласно настоящия регламент; и
 - ii) съдържат най-малко елементите, определени в приложение XII;
- в) въвеждат политика за спазване на правото на Съюза в областта на авторското право и сродните права, и по-специално с цел установяване и съобразяване, включително чрез най-съвременните технологии, на случаите на запазване на права съгласно член 4, параграф 3 от Директива (ЕС) 2019/790;
- г) представят и оповестяват публично достатъчно подробно обобщение на съдържанието, използвано за обучение на модела на ИИ с общо предназначение, по образец, осигурен от Службата по ИИ.

2. Задълженията, посочени в параграф 1, букви а) и б), не се прилагат за доставчиците на модели на ИИ, предоставени с безплатен лиценз с отворен код, който позволява достъп, използване, изменение и разпространение на модела, и чиито параметри, включително теглата, информацията за архитектурата на модела и информацията за използването на модела, са публично достъпни. Това изключение не се прилага за модели на ИИ с общо предназначение, пораждащи системни рискове.
3. Доставчиците на модели на ИИ с общо предназначение си сътрудничат при необходимост с Комисията и националните компетентни органи при упражняването на техните компетентност и правомощия съгласно настоящия регламент.
4. Доставчиците на модели на ИИ с общо предназначение могат да се основават на кодекси за добри практики по смисъла на член 56, за да покажат, че спазват задълженията по параграф 1 от настоящия член до публикуването на хармонизиран стандарт. По отношение на доставчиците, които спазват европейски хармонизиран стандарт, съществува презумпция за съответствие, доколкото стандартите обхващат посочените задължения. Доставчиците на модели на ИИ с общо предназначение, които не се придържат към одобрен кодекс за добри практики или не спазват европейски хармонизиран стандарт, представят други подходящи средства за постигане на съответствие с цел оценката им от Комисията.
5. С цел да се улесни спазването на приложение XI, и по-специално на точка 2, букви г) и д) от него, на Комисията се предоставя правомощието да приема делегирани актове в съответствие с член 97 с цел подробно описание на методиките за измерване и изчисляване, за да се даде възможност за съпоставима и проверяема документация.
6. На Комисията се предоставя правомощието приема делегирани актове в съответствие с член 97, параграф 2 с цел изменение на приложения XI и XII с оглед на технологичното развитие.
7. Всяка информация или документация, получена съгласно настоящия член, включително търговските тайни, се третира в съответствие със задълженията за поверителност, установени в член 78.

Член 54

Упълномощени представители на доставчиците на модели на ИИ с общо предназначение

1. Преди да пуснат модел на ИИ с общо предназначение на пазара на Съюза, доставчиците, установени в трети държави, с писмено пълномощно определят упълномощен представител, който е установен в Съюза.
2. Доставчикът осигурява възможност на упълномощения си представител да изпълнява задачите, посочени в пълномощното, получено от доставчика.
3. Упълномощеният представител изпълнява задачите, посочени в пълномощното, получено от доставчика. При поискване той предоставя на Службата по ИИ копие от пълномощното на един от официалните езици на институциите на Съюза. За целите на настоящия регламент пълномощното дава право на упълномощения представител да изпълнява следните задачи:
 - а) да проверява дали доставчикът е изготвил техническата документация, посочена в приложение XI, и дали е изпълнил всички задължения, установени в член 53, както и, когато е приложимо, в член 55;
 - б) да съхранява на разположение на Службата по ИИ и националните компетентни органи копие от техническата документация, посочена в приложение XI, в продължение на 10 години след пускането на модела на ИИ с общо предназначение на пазара, както и данни за контакт на доставчика, определил упълномощения представител;
 - в) да предоставя на Службата за ИИ, при обосновано искане, цялата информация и документация, включително посочената в буква б), необходима за доказване на спазването на задълженията по настоящата глава;
 - г) при мотивирано искане да си сътрудничи със Службата за ИИ и с компетентните органи относно всяко действие, което те предприемат във връзка с модела на ИИ с общо предназначение, включително когато моделът е интегриран в системи с ИИ, пуснати на пазара или пуснати в действие в Съюза.
4. Пълномощното дава право на упълномощения представител да отговаря, наред или вместо доставчика, пред Службата по ИИ или компетентните органи и засегнатите лица по всички въпроси, свързани с осигуряването на съответствие с настоящия регламент.

5. Упълномощеният представител се отказва от упълномощаването, ако счита или има основание да счита, че доставчикът действа в противоречие със задълженията си съгласно настоящия регламент. В такъв случай той също така незабавно информира Службата по ИИ за отказа от упълномощаването и основанията за това.

6. Задължението, установено в настоящия член, не се прилага за доставчиците на модели на ИИ с общо предназначение, предоставени с безплатен лиценз с отворен код, който позволява достъп, използване, изменение и разпространение на модела, и чиито параметри, включително теглата, информацията за архитектурата на модела и информацията за използването на модела, са публично достъпни, освен ако моделите на ИИ с общо предназначение не пораздават системни рискове.

РАЗДЕЛ 3

Задължения на доставчиците на модели на ИИ с общо предназначение, пораздащи системен риск

Член 55

Задължения на доставчиците на модели на ИИ с общо предназначение, пораздащи системен риск

1. В допълнение към задълженията, изброени в членове 53 и 54, доставчиците на модели на ИИ с общо предназначение, пораздащи системен риск:

- а) извършват оценка на модела в съответствие със стандартизирани протоколи и инструменти, отразяващи съвременните технологични постижения, включително провеждат и документират състезателно изпитване на модела с цел установяване и намаляване на системните рискове;
- б) оценяват и ограничават възможните системни рискове на равнището на Съюза, включително техните източници, които могат да произтичат от разработването, пускането на пазара или използването на модели на ИИ с общо предназначение, пораздащи системен риск;
- в) проследяват, документират и докладват без ненужно забавяне на Службата по ИИ и, когато е целесъобразно, на националните компетентни органи, съответната информация за сериозните инциденти и възможните коригиращи действия за справяне с тях;
- г) гарантират подходящо равнище на защита на киберсигурността за модела на ИИ с общо предназначение, пораздащ системен риск, и физическата инфраструктура на модела.

2. Доставчиците на модели на ИИ с общо предназначение, пораздащи системен риск, могат да се основават на кодекси за добри практики по смисъла на член 56, за да докажат спазването на задълженията по параграф 1 от настоящия член до публикуването на хармонизиран стандарт. По отношение на доставчиците, които спазват европейски хармонизиран стандарт, съществува презумпция за съответствие, доколкото стандартите обхващат посочените задължения. Доставчиците на модели на ИИ с общо предназначение, пораздащи системен риск, които не се придържат към одобрен кодекс за добри практики или не спазват европейски хармонизиран стандарт, представят други подходящи средства за постигане на съответствие с цел оценката им от Комисията.

3. Всяка информация или документация, получена съгласно настоящия член, включително търговските тайни, се третира в съответствие със задълженията за поверителност, установени в член 78.

РАЗДЕЛ 4

Кодекси за добри практики

Член 56

Кодекси за добри практики

- 1. Службата по ИИ насърчава и улеснява изготвянето на кодекси за добри практики на равнището на Съюза, за да се допринесе за правилното прилагане на настоящия регламент, като се вземат предвид международните подходи.
- 2. Службата по ИИ и Съветът по ИИ се стремят да гарантират, че кодексите за добри практики обхващат най-малко задълженията, предвидени в членове 53 и 55, включително следните въпроси:

- а) средствата за осигуряване на актуализиране на информацията, посочена в член 53, параграф 1, букви а) и б), с оглед на пазарното и технологичното развитие;
- б) степента на подробност на обобщението на съдържанието, използвано за обучение;
- в) установяването на вида и естеството на системните рискове на равнището на Съюза, включително техните източници, когато е целесъобразно;
- г) мерките, процедурите и условията за оценката и управлението на системните рискове на равнището на Съюза, включително свързаната с тях документация, като те трябва да са пропорционални на рисковете, съобразени с тяхната значимост и вероятност, както и с конкретните трудности за справяне с тези рискове с оглед на възможните начини, поради които те могат да възникнат и да се проявят по веригата за създаване на стойност в областта на ИИ.

3. Службата по ИИ може да покани всички доставчици на модели на ИИ с общо предназначение, както и съответните национални компетентни органи, да участват в изготвянето на кодекси за добри практики. Организациите на гражданското общество, стопанският сектор, академичните среди и други заинтересовани страни, като доставчици надолу по веригата и независими експерти, могат да подкрепят процеса.

4. Службата по ИИ и Съветът по ИИ се стремят да гарантират, че в кодексите за добри практики ясно се определят техните конкретни цели и се съдържат ангажименти или мерки, включително, когато е целесъобразно, ключови показатели за ефективност, за да могат да се постигнат тези цели, и че в тях надлежно се вземат предвид потребностите и интересите на всички заинтересовани страни, включително засегнатите лица, на равнището на Съюза.

5. Службата по ИИ се стреми да гарантира, че придържащите се към кодексите за добри практики докладват редовно на Службата по ИИ относно изпълнението на ангажиментите и предприетите мерки и резултатите от тях, включително измерени спрямо ключовите показатели за изпълнение, когато е целесъобразно. В ключовите показатели за изпълнение и ангажиментите за докладване се отчитат разликите между различните участници от гледна точка на размер и капацитет.

6. Службата по ИИ и Съветът по ИИ редовно наблюдават и оценяват постигането на целите, заложи в кодексите за добри практики, от страна на участниците и техния принос за правилното прилагане на настоящия регламент. Службата по ИИ и Съветът по ИИ оценяват дали кодексите за добри практики обхващат задълженията, предвидени в членове 53 и 55, и редовно наблюдават и оценяват постигането на заложените в тях цели. Те публикуват своята оценка на адекватността на кодексите за добри практики.

Комисията може да одобри чрез акт за изпълнение даден кодекс за добри практики и да осигури общата му приложимост в рамките на Съюза. Този акт за изпълнение се приема в съответствие с процедурата по разглеждане, посочена в член 98, параграф 2.

7. Службата по ИИ може да прикани всички доставчици на модели на ИИ с общо предназначение да се придържат към кодексите за добри практики. За доставчиците на модели на ИИ с общо предназначение, които не пораждаат системни рискове, придържането може да бъде ограничено до задълженията, предвидени в член 53, освен ако те изрично не заявят интерес да се придържат изцяло към кодекса.

8. Когато е целесъобразно, Службата по ИИ насърчава и улеснява прегледа и адаптирането на кодексите за добри практики, по-специално с оглед на нови стандарти. Службата по ИИ подпомага оценката на наличните стандарти.

9. Кодексите за добри практики трябва да са готови до 2 май 2025 г. Службата по ИИ предприема необходимите мерки, включително отправя покана към доставчиците съгласно параграф 7.

Ако до 2 август 2025 г., даден кодекс за добри практики не може да бъде подготвен или ако Службата по ИИ счете, че той не е подходящ съгласно оценката му по параграф 6 от настоящия член, Комисията може да предвиди чрез актове за изпълнение общи правила за изпълнението на задълженията, предвидени в членове 53 и 55, включително въпросите, посочени в параграф 2 от настоящия член. Тези актове за изпълнение се приемат в съответствие с процедурата по разглеждане, посочена в член 98, параграф 2.

ГЛАВА VI
МЕРКИ В ПОДКРЕПА НА ИНОВАЦИИТЕ

Член 57

Регулаторни лаборатории в областта на ИИ

1. Държавите членки гарантират, че техните компетентни органи създават най-малко една регулаторна лаборатория в областта на ИИ на национално равнище, която започва да функционира до 2 август 2026 г. Тази лаборатория може също да бъде създадена съвместно с компетентните органи на други държави членки. Комисията може да предоставя техническа подкрепа, консултации и инструменти за създаването и функционирането на регулаторни лаборатории в областта на ИИ.

Задължението по първа алинея може да бъде изпълнено и чрез участие в съществуваща лаборатория, доколкото това участие осигурява равностойно равнище на национално покритие за участващите държави членки.

2. Могат да бъдат създадени и допълнителни регулаторни лаборатории в областта на ИИ на регионално или местно равнище или съвместно с компетентните органи на други държави членки.

3. Европейският надзорен орган по защита на данните може също така да създаде регулаторна лаборатория в областта на ИИ за институциите, органите, службите и агенциите на Съюза и да изпълнява функциите и задачите на националните компетентни органи в съответствие с настоящата глава.

4. Държавите членки гарантират, че компетентните органи, посочени в параграфи 1 и 2, заделят достатъчно ресурси за ефективното и своевременно спазване на настоящия член. Когато е целесъобразно, националните компетентни органи си сътрудничат с други съответни органи и могат да допуснат включването на други участници в екосистемата на ИИ. Настоящият член не засяга други регулаторни лаборатории, създадени съгласно правото на Съюза или националното право. Държавите членки гарантират подходящо равнище на сътрудничество между органите, упражняващи надзор върху тези други лаборатории, и националните компетентни органи.

5. Регулаторните лаборатории в областта на ИИ, създадени съгласно параграф 1, осигуряват контролирана среда, която насърчава иновациите и улеснява разработването, обучението, изпитването и валидирането на иновативни системи с ИИ в рамките на ограничен срок, преди те да бъдат пуснати на пазара или в действие съгласно конкретен план за лаборатория, договорен между доставчиците или потенциалните доставчици и компетентния орган. Тези лаборатории могат да включват изпитване в реални условия, върху което се упражнява надзор в рамките на лабораторията.

6. Компетентните органи осигуряват, когато е целесъобразно, насоки, надзор и подкрепа в рамките на регулаторната лаборатория в областта на ИИ с цел установяване на рисковете, по-специално по отношение на основните права, здравето и безопасността, изпитванията, мерките за смекчаване на последиците и тяхната ефективност във връзка със задълженията и изискванията на настоящия регламент и, когато е приложимо, на друго право на Съюза и национално право, във връзка с което се упражнява надзор в рамките на лабораторията.

7. Компетентните органи дават на доставчиците и на потенциалните доставчици, участващи в регулаторна лаборатория в областта на ИИ, насоки относно регулаторните очаквания и начините за изпълнение на изискванията и задълженията, установени в настоящия регламент.

При поискване от доставчика или потенциалния доставчик на системата с ИИ компетентният орган изготвя писмено доказателство за успешно извършените дейности в лабораторията. Компетентният орган също така изготвя доклад за напускане, в който подробно се описват дейностите, извършени в лабораторията, и свързаните с тях общи резултати и резултати от обучението. Доставчиците могат да използват тази документация, за да докажат съответствието си с настоящия регламент по време на процеса на оценяване на съответствието или съответните дейности по надзор на пазара. Във връзка с това докладите за напускане и писмените доказателства, изготвени от националния компетентен орган, се вземат предвид от органите за надзор на пазара и нотифицираните органи с оглед ускоряване на процедурите за оценяване на съответствието в разумна степен.

8. При спазване на разпоредбите за поверителност на член 78 и със съгласието на доставчика или потенциалния доставчик, на Комисията и Съвета по ИИ се разрешава достъп до докладите за напускане. Те ги вземат предвид, когато е целесъобразно, при изпълнението на своите задачи съгласно настоящия регламент. Ако както доставчикът или потенциалният доставчик, така и националният компетентен орган изрично дадат съгласието си, докладът за напускане може да бъде оповестен публично чрез единната информационна платформа, посочена в настоящия член.

9. Създаването на регулаторни лаборатории в областта на ИИ има за цел да допринесе за постигането на следните цели:

а) подобряване на правната сигурност за постигане на регулаторно съответствие с настоящия регламент или, когато е приложимо, с друго приложимо право на Съюза и национално право;

- б) подпомагане на обмена на добри практики чрез сътрудничество с органите, участващи в регулаторните лаборатории в областта на ИИ;
- в) насърчаване на иновациите и конкурентоспособността и улесняване на развитието на екосистема на ИИ;
- г) спомагане за основаното на факти натрупване на регулаторен опит.
- д) улесняване и ускоряване на достъпа до пазара на Съюза за системи с ИИ, по-специално когато те се предоставят МСП, включително новосъздадени предприятия.

10. Националните компетентни органи 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 или компетентни органи са привлечени във функционирането на регулаторната лаборатория в областта на ИИ и участват в надзора на онези аспекти, които контролират в рамките на съответните си задачи и правомощия.

11. Регулаторните лаборатории в областта на ИИ не засягат надзорните или коригиращите правомощия на компетентните органи, упражняващи надзор върху регулаторните лаборатории, включително на регионално или местно равнище. Всички значителни рискове за здравето и безопасността и за основните права, набелязани по време на разработването и изпитването на такива системи с ИИ, трябва да водят до предприемането подходящи ограничителни мерки. Националните компетентни органи трябва да разполагат с правомощието да спрат или да прекратят процеса на изпитване или участието в лабораторията, ако не е възможно ефективно въвеждане на ограничителните мерки, и да информират Службата по ИИ за това решение. Тези органи упражняват своите надзорни правомощия в рамките на съответното право, като използват свободата си на преценка при прилагане на нормативни разпоредби по отношение на конкретен проект за регулаторна лаборатория в областта на ИИ, с цел подкрепа на иновациите в областта на ИИ в Съюза.

12. Доставчиците и потенциалните доставчици, участващи в регулаторната лаборатория в областта на ИИ продължават да носят отговорност съгласно приложимото право на Съюза и национално право относно отговорността за всяка вреда, причинена на трети лица в резултат от експериментите, провеждани в лабораторията. Въпреки това, при условие че потенциалните доставчици спазват конкретните план и условия за участие и добросъвестно следват указанията, дадени от националния компетентен орган, органите не налагат административни глоби и имуществени санкции за нарушения на настоящия регламент. Когато други компетентни органи, отговарящи за други области на правото на Съюза и на националното право, са участвали активно в надзора на системата с ИИ в регулаторната лаборатория и са дали насоки за осигуряване на спазването му, по отношение на това право не се налагат административни глоби и имуществени санкции.

13. Регулаторните лаборатории в областта на ИИ се проектират и изграждат по такъв начин, че когато е целесъобразно, да улесняват трансграничното сътрудничество между националните компетентни органи.

14. Националните компетентни органи координират своите дейности и си сътрудничат в рамките на Съвета по ИИ.

15. Националните компетентни органи информират Службата по ИИ и Съвета по ИИ за създаването на лаборатория и могат да поискат от тях подкрепа и насоки. Службата по ИИ оповестява публично списък на планираните и съществуващите лаборатории и го актуализира, за да насърчи по-голямото взаимодействие в регулаторните лаборатории в областта на ИИ и трансграничното сътрудничество.

16. Националните компетентни органи представят на Службата по ИИ и на Съвета по ИИ годишни доклади, за първи път една година след създаването на регулаторната лаборатория и ежегодно след това до нейното закриване, както и окончателен доклад. В тези доклади се предоставя информация за напредъка и резултатите от дейността на тези лаборатории, включително за най-добри практики, инциденти, извлечени поуки и препоръки за тяхното създаване и, когато е целесъобразно, за прилагането и евентуалното преразглеждане на настоящия регламент, включително свързаните с него делегирани актове и актове за изпълнение, и за прилагането на друго право на Съюза, във връзка с което се упражнява надзор от компетентните органи в рамките на лабораторията. Националните компетентни органи предоставят на обществеността достъп до тези годишни доклади или техни обобщения онлайн. Когато е целесъобразно, Комисията взема предвид годишните доклади при изпълнението на своите задачи съгласно настоящия регламент.

17. Комисията разработва единен и специализиран интерфейс, съдържащ цялата съответна информация, свързана с регулаторните лаборатории в областта на ИИ, за да даде възможност на заинтересованите страни да взаимодействат с регулаторните лаборатории и да отправят запитвания до компетентните органи, и да търсят необвързващи насоки относно съответствието на иновативни продукти, услуги и бизнес модели, в които са вградени технологии на ИИ, в съответствие с член 62, параграф 1, буква в). Комисията активно координира действията си с националните компетентни органи, когато е приложимо.

Член 58

Подробни правила за регулаторните лаборатории в областта на ИИ и тяхното функциониране

1. За да се избегне разпокъсаността в рамките на Съюза, Комисията приема актове за изпълнение, в които се съдържат подробните правила за създаване, разработване, внедряване, функциониране и надзор на регулаторните лаборатории в областта на ИИ. Актовете за изпълнение включват общи принципи по следните въпроси:

- а) допустимостта и критериите за подбор за участие в регулаторната лаборатория в областта на ИИ;
- б) процедурите за подаване на заявления, за участие, за мониторинг, за напускане и за прекратяване на дейността на регулаторната лаборатория в областта на ИИ, включително плана за регулаторната лаборатория и доклада за напускане;
- в) реда и условията, приложими за участниците.

Тези актове за изпълнение се приемат в съответствие с процедурата по разглеждане, посочена в член 98, параграф 2.

2. Посочените в параграф 1 актове за изпълнение гарантират, че:

- а) в регулаторните лаборатории в областта на ИИ е възможно участието на всеки кандидатстващ доставчик или потенциален доставчик на система с ИИ, който отговаря на критериите за допустимост и подбор, които трябва да са прозрачни и справедливи, и че националните компетентни органи информират заявителите за своето решение в срок от три месеца от подаването на заявлението;
- б) регулаторните лаборатории в областта на ИИ осигуряват широк и равен достъп и са съобразени с нивото на търсене на участие; доставчиците и потенциалните доставчици могат също така да подават заявления в партньорства с внедрителите и други съответни трети лица;
- в) подробните правила и условия относно регулаторните лаборатории в областта на ИИ подкрепят във възможно най-голяма степен гъвкавостта на националните компетентни органи да създават и управляват своите регулаторни лаборатории в областта на ИИ;
- г) достъпът до регулаторните лаборатории в областта на ИИ е безплатен за МСП, включително новосъздадените предприятия, без да се засягат извънредните разходи, които националните компетентни органи могат да възстановят по справедлив и пропорционален начин;
- д) те улесняват доставчиците и потенциалните доставчици, посредством резултатите от самообучението на регулаторните лаборатории в областта на ИИ, при изпълнението на задълженията за оценяване на съответствието по настоящия регламент и при прилагането на доброволна основа на кодексите за поведение, посочени в член 95;
- е) регулаторните лаборатории улесняват участието на други съответни участници в екосистемата на ИИ, като нотифицирани органи и организации за стандартизация, МСП, включително новосъздадени предприятия, предприятия, новатори, структури за изпитване и експериментиране, лаборатории за научни изследвания и експериментиране и европейски центрове за цифрови иновации, центрове за високи постижения, отделни научни работници, за да се позволи и улесни сътрудничеството с публичния и частния сектор;
- ж) процедурите, процесите и административните изисквания за кандидатстване, подбор, участие и напускане на регулаторната лаборатория в областта на ИИ са прости, лесно разбираеми, ясно съобщени, за да се улесни участието на МСП, включително новосъздадени предприятия, с ограничен правен и административен капацитет, и са рационализирани в целия Съюз, за да се избегне разпокъсаност, и че участието в регулаторна лаборатория в областта на ИИ, създадена от държава членка или от Европейския надзорен орган за защита на данните, е взаимно и еднакво признато и има еднакви правни последици в целия Съюз;
- з) участието в регулаторната лаборатория в областта на ИИ се ограничава до срок, който съответства на сложността и мащаба на проекта и който може да бъде удължен от националния компетентен орган;
- и) регулаторните лаборатории в областта на ИИ улесняват разработването на инструменти и инфраструктура за изпитване, сравнителен анализ, оценяване и разясняване на измеренията на системите с ИИ, свързани с регулаторно самообучение, като точност, надеждност и киберсигурност, както и мерки за смекчаване на рисковете за основните права и обществото като цяло.

3. Потенциалните доставчици на услуги в регулаторните лаборатории в областта на ИИ, по-специално на МСП и новосъздадените предприятия, биват насочвани, когато е целесъобразно, до услуги на етапа преди внедряването, като например насоки относно прилагането на настоящия регламент, до други услуги с добавена стойност, като например помощ при изготвянето на документи за стандартизация и сертифициране, съоръжения за изпитване и експериментиране, европейски центрове за цифрови иновации и центрове за високи постижения.

4. Когато националните компетентни органи разглеждат възможността да разрешат изпитване в реални условия, върху което се упражнява надзор в рамките на регулаторна лаборатория за ИИ, създадена съгласно настоящия член, те постигат изрична договореност с участниците относно реда и условията на това изпитване, и по-специално относно подходящите гаранции с оглед на защитата на основните права, здравето и безопасността. Когато е целесъобразно, те си сътрудничат с други национални компетентни органи с цел да се осигурят съгласувани практики в целия Съюз.

Член 59

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

1. Личните данни, събрани законно за други цели, може да бъдат обработвани в регулаторна лаборатория в областта на ИИ само с цел разработване, обучение и изпитване на някои системи с ИИ в лабораторията, когато са изпълнени всички посочени по-долу условия:

- a) системите с ИИ се разработват за защита на значителен обществен интерес от публичен орган или друго физическо или юридическо лице и в една или повече от следните области:
 - i) обществена безопасност и обществено здраве, включително откриване, диагностициране, профилактика, контрол и лечение на болести и подобряване на системите за здравеопазване;
 - ii) високо равнище на опазване и подобряване на качеството на околната среда, защита на биологичното разнообразие, защита срещу замърсяването, мерки за екологичен преход, смекчаване на последиците и адаптиране към изменението на климата;
 - iii) енергийна устойчивост;
 - iv) безопасност и устойчивост на транспортните системи и мобилността, критичната инфраструктура и мрежите;
 - v) ефикасност и качество на публичната администрация и публичните услуги;
- б) обработваните данни са необходими за съответствие с едно или повече от изискванията, посочени в глава III, раздел 2, когато тези изисквания не могат да бъдат ефективно изпълнени чрез обработването на анонимизирани, синтетични или други нелични данни;
- в) съществуват ефективни механизми за мониторинг, за да се установи дали по време на експериментирането в лабораторията могат да възникнат високи рискове за правата и свободите на субектите на данни, посочени в член 35 от Регламент (ЕС) 2016/679 и в член 39 от Регламент (ЕС) 2018/1725, както и механизми за реагиране с цел бързо смекчаване на тези рискове и, при необходимост, прекратяване на обработването;
- г) всички лични данни, които се обработват в контекста на лабораторията, са във функционално отделна, изолирана и защитена среда за обработване на данни под контрола на потенциалния доставчик и до тези данни само имат достъп оправомощени лица;
- д) доставчиците могат да споделят допълнително първоначално събраните данни само в съответствие с правото на Съюза за защита на данните; съхранявани в лабораторията лични данни не могат да бъдат споделяни извън нея;
- е) обработването на лични данни в контекста на лабораторията не води до мерки или решения, засягащи субектите на данни, нито засяга прилагането на техните права, установени в правото на Съюза относно защитата на личните данни;
- ж) всички лични данни, обработвани в контекста на лабораторията, са защитени чрез подходящи технически и организационни мерки и се заличават, след като участието в нея приключи или изтече срокът на съхранение на личните данни;
- з) записите за обработването на лични данни в контекста на лабораторията се съхраняват за срока на участие в нея, освен ако в правото на Съюза или националното право не е предвидено друго;
- и) пълното и подробно описание на процеса и обосновката за обучаването, изпитването и валидирането на системата с ИИ се съхранява заедно с резултатите от изпитванията като част от техническата документация, посочена в приложение IV;

й) кратко обобщение на проекта за ИИ, разработен в лабораторията, неговите цели и очаквани резултати се публикуват на уебсайта на компетентните органи; това задължение не обхваща чувствителни оперативни данни във връзка с дейностите на правоохранителните органи, органите за граничен контрол, имиграционните органи или органите в областта на убежището.

2. За целите на предотвратяването, разследването, откриването или наказателното преследване на престъпления или на изпълнението на наказателноправни санкции, включително на предотвратяването на заплахи за обществената сигурност и тяхното предотвратяване, под контрола и отговорността на правоохранителните органи, обработването на лични данни в регулаторни лаборатории в областта на ИИ се основава на специалното право на Съюза или национално право, като се прилагат същите кумулативни условия като посочените в параграф 1.

3. Параграф 1 не засяга правото на Съюза или националното право, което изключва обработването на лични данни за цели, различни от изрично посочените в това право, както и правото на Съюза или националното право, с което се определя основанието за обработването на лични данни, необходимо за целите на разработването, изпитването или обучението на иновативни системи с ИИ, или всяко друго правно основание, което е в съответствие с правото на Съюза в областта на защитата на личните данни.

Член 60

Изпитване на високорискови системи с ИИ в реални условия извън регулаторните лаборатории в областта на ИИ

1. Изпитването на високорискови системи с ИИ в реални условия извън регулаторните лаборатории в областта на ИИ може да се извършва от доставчици или потенциални доставчици на високорискови системи с ИИ, изброени в приложение III, в съответствие с настоящия член и плана за изпитване в реални условия, посочен в настоящия член, без да се засягат забраните съгласно член 5.

Комисията чрез актове за изпълнение конкретизира подробните елементи на плана за изпитване в реални условия. Тези актове за изпълнение се приемат в съответствие с процедурата по разглеждане, посочена в член 98, параграф 2.

Настоящият параграф не засяга правото на Съюза или националното право относно изпитването в реални условия на високорискови системи с ИИ, свързани с продукти, които са обхванати от законодателството на Съюза за хармонизация, посочено в приложение I.

2. Доставчиците или потенциалните доставчици могат да провеждат изпитвания на високорискови системи с ИИ, посочени в приложение III, в реални условия по всяко време преди пускането на пазара или пускането в действие на системата с ИИ, самостоятелно или в партньорство с един или повече внедрители или потенциални внедрители.

3. Изпитването на високорискови системи с ИИ в реални условия съгласно настоящия член не засяга оценките на съответствието с етичните стандарти, които може да се изискват съгласно правото на Съюза или националното право.

4. Доставчиците или потенциалните доставчици могат да извършват изпитването в реални условия само когато са изпълнени всички посочени по-долу условия:

- а) доставчикът или потенциалният доставчик е изготвил план за изпитване в реални условия и го е представил на органа за надзор на пазара в държавата членка, в която ще се извърши изпитването в реални условия;
- б) органът за надзор на пазара в държавата членка, в която ще се извърши изпитването в реални условия, е одобрил изпитването в реални условия и плана за изпитване в реални условия; когато органът за надзор на пазара не е дал отговор в рамките на 30 дни, изпитването в реални условия и планът за изпитване в реални условия се считат за одобрени; когато националното право не предвижда мълчаливо одобрение, за изпитването в реални условия продължава да се изисква разрешение;
- в) доставчикът или потенциалният доставчик — с изключение на доставчиците или потенциалните доставчици на високорискови системи с ИИ, посочени в точки 1, 6 и 7 от приложение III, в правоохранителната област и в областта на управлението на миграцията, убежището и граничния контрол, и на високорисковите системи с ИИ, посочени в точка 2 от приложение III — е регистрирал изпитването в реални условия в съответствие с член 71, параграф 4, с уникален единен идентификационен номер в рамките на Съюза и с информацията, посочена в приложение IX; доставчикът или потенциалният доставчик на високорискови системи с ИИ, посочени в точки 1, 6 и 7 от приложение III, в правоохранителната област и в областта на управлението на миграцията, убежището и граничния контрол е регистрирал изпитването в реални условия в защитения непубличен раздел от базата данни на ЕС в съответствие с член 49, параграф 4, буква г), с уникален единен идентификационен номер в рамките на Съюза и с информацията, посочена в същата разпоредба; доставчикът или потенциалният доставчик на високорискови системи с ИИ, посочени в точка 2 от приложение III, е регистрирал изпитването в реални условия в съответствие с член 49, параграф 5;

- г) доставчикът или потенциалният доставчик, който извършва изпитването в реални условия, е установен в Съюза или е определил представител, който е установен в Съюза;
 - д) данните, които се събират и обработват за целите на изпитването в реални условия, се предават на трети лица само ако се прилагат подходящи и приложими гаранции съгласно правото на Съюза;
 - е) изпитването в реални условия не продължава по-дълго от необходимото за постигане на целите му и във всеки случай не повече от шест месеца, като този срок може да бъде удължен с още шест месеца, при условие че доставчикът или потенциалният доставчик уведоми предварително органа за надзор на пазара и приложи обяснение за необходимостта от такова удължаване;
 - ж) участниците в изпитването в реални условия, които са лица, принадлежащи към уязвими групи, поради своята възраст или увреждане, са защитени по подходящ начин;
 - з) когато доставчик или потенциален доставчик организира изпитването в реални условия в сътрудничество с един или повече внедрители или потенциални внедрители, последните са информирани за всички аспекти на изпитването, които са от значение за решението им да участват, и са получили съответните инструкции за употреба на системата с ИИ, посочени в член 13; доставчикът или потенциалният доставчик и внедрителят или потенциалният внедрител сключват споразумение, в което се определят функциите и отговорностите им с цел да се гарантира спазването на разпоредбите за изпитване в реални условия съгласно настоящия регламент и друго приложимо право на Съюза и национално право;
 - и) субектите в изпитването в реални условия са дали информирано съгласие в съответствие с член 61 или - в свързани със правоохранителната област случаи, когато търсенето на информирано съгласие би попречило на изпитването на системата с ИИ - изпитването и резултатите от него не оказват никакво отрицателно въздействие върху субектите в изпитването и техните лични данни се заличават след провеждането на изпитването;
 - й) изпитването в реални условия се контролира ефективно от доставчика или потенциалния доставчик, както и от внедрителя или потенциалния внедрител чрез лица, които имат подходящата квалификация в съответната област и разполагат с необходимия капацитет, обучение и авторитет за изпълнение на своите задачи;
 - к) прогнозите, препоръките или решенията, генерирани от системата с ИИ, могат ефективно да се отменят и пренебрегнат.
5. Всички субекти в изпитването в реални условия или техните законно определени представители, в зависимост от случая, може, без това да навреди по никакъв начин и без да е необходимо да представят обосновка, да се оттеглят от изпитването по всяко време, като оттеглят своето информирано съгласие и поискат незабавно и окончателно заличаване на личните им данни. Оттеглянето на информираното съгласие не засяга извършените дейности.
6. В съответствие с член 75 държавите членки предоставят на своите органи за надзор на пазара правомощията да изискват от доставчиците и потенциалните доставчици да предоставят информация, да извършват внезапни дистанционни проверки или проверки на място, както и проверки на провеждането на изпитванията в реални условия и на свързаните с тях високорискови системи с ИИ. Органите за надзор на пазара упражняват тези правомощия, за да гарантират безопасното разработване на изпитването в реални условия.
7. Всеки сериозен инцидент, установен по време на изпитването в реални условия, се докладва на националния орган за надзор на пазара в съответствие с член 73. Доставчикът или потенциалният доставчик предприема незабавни мерки за смекчаване на последиците или, ако това не е възможно, спира изпитването в реални условия, докато не бъдат предприети такива мерки, или го прекратява по друг начин. Доставчикът или потенциалният доставчик установява процедура за бързо изземване на системата с ИИ при прекратяването на изпитването в реални условия.
8. Доставчиците или потенциалните доставчици уведомяват националния орган за надзор на пазара в държавата членка, където ще се проведе изпитването в реални условия, за спирането или прекратяването на изпитването в реални условия и за крайните резултати.
9. Доставчикът или потенциалният доставчик носят отговорност съгласно приложимото право на Съюза и национално право за всяка вреда, причинена в хода на изпитването в реални условия.

Член 61

Информирано съгласие за участие в изпитване в реални условия извън регулаторните лаборатории в областта на ИИ

1. За целите на изпитването в реални условия съгласно член 60 субектите в изпитването изразяват свободно информираното си съгласие, преди да вземат участие в изпитването и след като са били надлежно информирани чрез кратка, ясна, подходяща и разбираема информация относно:

- а) естеството и целите на изпитването в реални условия и евентуалните неудобства, които могат да произтекат от участието им;
- б) условията, в които ще се извърши изпитването в реални условия, включително очакваната продължителност на участието на субекта или субектите в изпитването;
- в) правата и гаранциите относно участието им, и по-специално правото им да откажат да участват и правото да напуснат изпитването в реални условия по всяко време, без това да води до неблагоприятни за тях последици и без да е необходимо да дават обяснение;
- г) условията за искане на отмяна или пренебрегване на прогнозите, препоръките или решенията, генерирани от системата с ИИ;
- д) уникалния единен идентификационен номер в рамките на Съюза на изпитването в реални условия в съответствие с член 60, параграф 4, буква в), и данните за контакт на доставчика или неговия представител, от когото може да бъде получена допълнителна информация.

2. Информираното съгласие се оформя като документ с указана дата, като на субектите в изпитването или на техния представител се предоставя копие.

Член 62

Мерки за доставчици и внедрители, по-специално МСП, включително новосъздадени предприятия

1. Държавите членки предприемат следните действия:

- а) осигуряват на МСП, включително новосъздадени предприятия, които имат седалище или клон в Съюза, приоритетен достъп до регулаторните лаборатории в областта на ИИ, доколкото те отговарят на условията за допустимост и подбор; приоритетният достъп не изключва достъпа на други МСП, включително новосъздадени предприятия, различни от посочените в настоящия параграф, до регулаторната лаборатория в областта на ИИ, при условие че отговарят на условията за допустимост и критериите за подбор;
- б) организират специфични дейности за повишаване на осведомеността и обучение относно прилагането на настоящия регламент, съобразени с нуждите на МСП, включително новосъздадените предприятия, внедрителите и, когато е целесъобразно, органите на местна власт;
- в) използват съществуващите специални канали и когато е целесъобразно, създават нови канали за комуникация с МСП, включително новосъздадените предприятия, внедрителите, други новатори и, когато е целесъобразно, с органите на местна власт, за да предоставят консултации и да отговарят на запитвания относно прилагането на настоящия регламент, включително относно участието в регулаторни лаборатории в областта на ИИ;
- г) улесняват участието на МСП и други съответни заинтересовани страни в процеса на разработване на стандарти.

2. При определянето на таксите за оценяване на съответствието съгласно член 43 се вземат предвид особените интереси и нужди на доставчиците, които са МСП, включително новосъздадени предприятия, като тези такси се намаляват пропорционално на техния размер, размера на пазара и други относими показатели.

3. Службата по ИИ предприема следните действия:

- а) осигурява стандартизирани образци за обхванатите от настоящия регламент области, посочени от Съвета по ИИ в искането му;
- б) разработва и поддържа единна информационна платформа, осигуряваща лесна за използване информация във връзка с настоящия регламент за всички оператори в Съюза;

- в) организира подходящи комуникационни кампании за повишаване на осведомеността относно задълженията, произтичащи от настоящия регламент;
- г) оценява и насърчава сближаването на най-добрите практики, прилагани в рамките на процедурите за възлагане на обществени поръчки във връзка със системите с ИИ.

Член 63

Дерогации за конкретни оператори

1. Микропредприятията по смисъла на Препоръка 2003/361/ЕО могат да спазват по опростен начин изискванията относно определени елементи на системата за управление на качеството, изисквана съгласно член 17 от настоящия регламент, при условие че нямат предприятия партньори или свързани предприятия по смисъла на посочената препоръка. За тази цел Комисията разработва насоки относно елементите на системата за управление на качеството, във връзка с които е възможно спазване по опростен начин, като се вземат предвид нуждите на микропредприятията, без да се засяга равнището на защита или необходимостта от спазване на изискванията относно високорисковите системи с ИИ.
2. Параграф 1 от настоящия член не се тълкува като освобождаващ посочените оператори от изпълнението на други изисквания и задължения, предвидени в настоящия регламент, включително установените в членове 9, 10, 11, 12, 13, 14, 15, 72 и 73.

ГЛАВА VII

УПРАВЛЕНИЕ

РАЗДЕЛ 1

Управление на равнището на Съюза

Член 64

Служба по ИИ

1. Комисията развива експертния опит и способностите на Съюза в областта на ИИ чрез Службата по ИИ.
2. Държавите членки улесняват изпълнението на задачите, възложени на Службата за ИИ, както е отразено в настоящия регламент.

Член 65

Създаване и структура на Европейския съвет по изкуствен интелект

1. Създава се Европейски съвет по изкуствен интелект (наричан по-долу „Съветът по ИИ“).
2. Съветът по ИИ се състои от по един представител на всяка държава членка. Европейският надзорен орган по защита на данните участва като наблюдател. Службата по ИИ също присъства на заседанията на Съвета по ИИ, без да участва в гласуването. Съветът по ИИ може да кани на заседанията си други национални органи, структури или експерти или органи, структури или експерти на Съюза, в зависимост от конкретния случай, когато обсъжданите въпроси са от значение за тях.
3. Всеки представител се определя от съответната държава членка за срок от три години, който може да бъде подновен еднократно.
4. Държавите членки гарантират, че представителите им в Съвета по ИИ:
 - а) притежават необходимите компетентност и правомощия в своята държава членка, за да могат да допринасят активно за изпълнението на задачите на Съвета по ИИ, посочени в член 66;
 - б) са определени като единно звено за контакт по отношение на Съвета по ИИ и, когато е целесъобразно предвид потребностите на държавите членки, като единно звено за контакт за заинтересованите страни;

в) разполагат с правомощия за улесняване на съгласуваността и координацията между националните компетентни органи в своята държава членка по отношение на прилагането на настоящия регламент, включително чрез събиране на съответните данни и информация с цел изпълнението на задачите им в рамките на Съвета по ИИ.

5. Определените представители на държавите членки приемат процедурен правилник на Съвета по ИИ с мнозинство от две трети. В процедурния правилник се установяват по-специално процедурите в рамките на процеса на подбор, продължителността на мандата и характеристиките на задачите на председателя, подробните правила за гласуване и организацията на дейностите на Съвета по ИИ и на неговите подгрупи.

6. Съветът по ИИ създава две постоянни подгрупи, които да осигуряват платформа за сътрудничество и обмен между органите за надзор на пазара и нотифициращите органи по въпроси, свързани съответно с надзора на пазара и нотифицираните органи.

Постоянната подгрупа за надзор на пазара следва да работи във връзка с настоящия регламент като група за административно сътрудничество (ADCO) по смисъла на член 30 от Регламент (ЕС) 2019/1020.

Съветът по ИИ може да създаде други постоянни или временни подгрупи, когато това е целесъобразно за разглеждането на конкретни въпроси. Когато е целесъобразно, представителите на консултативния форум, посочен в член 67, могат да бъдат поканени в тези подгрупи или на конкретни техни заседания в качеството на наблюдатели.

7. Съветът по ИИ е организиран и работи по такъв начин, че да се запазят обективността и безпристрастността на неговата дейност.

8. Съветът по ИИ се председателства от един от представителите на държавите членки. Службата по ИИ осигурява секретариата на Съвета по ИИ, свиква заседанията по искане на председателя и подготвя дневния ред в съответствие със задачите на Съвета по ИИ съгласно настоящия регламент и процедурния му правилник.

Член 66

Задачи на Съвета по ИИ

Съветът по ИИ консултира и подпомага Комисията и държавите членки за улесняване на последователното и ефективно прилагане на настоящия регламент. За тази цел Съветът по ИИ може по-специално:

- а) да допринася за координацията между националните компетентни органи, отговарящи за прилагането на настоящия регламент, и - в сътрудничество и със съгласието на съответните органи за надзор на пазара – да подкрепя съвместните дейности на органите за надзор на пазара, посочени в член 74, параграф 11;
- б) да събира и обменя технически и регулаторен експертен опит и най-добри практики между държавите членки;
- в) да дава консултации при прилагането на настоящия регламент, по-специално по отношение на прилагането на правилата относно моделите на ИИ с общо предназначение;
- г) да допринася за хармонизирането на административните практики в държавите членки, включително по отношение на дерогацията от процедурите за оценяване на съответствието, посочени в член 46, функционирането на регулаторните лаборатории в областта на ИИ и изпитването в реални условия, посочени в членове 57, 59 и 60;
- д) по искане на Комисията или по своя собствена инициатива да отправя препоръки и писмени становища по всички относими въпроси, свързани с изпълнението на настоящия регламент и неговото последователно и ефективно прилагане, включително:
 - i) относно разработването и прилагането на кодекси за поведение и кодекси за добри практики съгласно настоящия регламент, както и насоките на Комисията;
 - ii) оценката и прегледа на настоящия регламент съгласно член 112, включително по отношение на докладите за сериозни инциденти, посочени в член 73, и функционирането на базата данни на ЕС, посочена в член 71, изготвянето на делегираните актове или актовете за изпълнение, както и по отношение на евентуалното привеждане в съответствие на настоящия регламент със законодателството на Съюза за хармонизация, посочено в приложение I;
 - iii) относно техническите спецификации или съществуващите стандарти по отношение на изискванията, установени в глава III, раздел 2;

- iv) относно използването на хармонизираните стандарти или общите спецификации, посочени в членове 40 и 41;
 - v) тенденциите, като например европейската конкурентоспособност в световен мащаб в областта на ИИ, навлизането на ИИ в Съюза и развитието на цифровите умения;
 - vi) тенденциите по отношение на променящата се типология на веригите за създаване на стойност в областта на ИИ, по-специално по отношение на произтичащите от това последици по отношение на отчетността;
 - vii) относно евентуалната необходимост от изменение на приложение III в съответствие с член 7 и относно евентуалната необходимост от преразглеждане на член 5 съгласно член 112, като взема предвид съответните налични данни и най-новото в развитието на технологиите;
- е) да подкрепя Комисията в насърчаването на грамотността в областта на ИИ, обществената осведоменост и разбиране за ползите, рисковете, гаранциите и правата и задълженията, свързани с използването на системи с ИИ;
 - ж) да улеснява разработването на общи критерии и споделено разбиране сред пазарните оператори и компетентните органи на съответните понятия, предвидени в настоящия регламент, включително като допринася за разработването на сравнителни показатели;
 - з) да си сътрудничи, когато е целесъобразно, с други институции, органи, служби и агенции на Съюза, както и съответни експертни групи и мрежи на Съюза, по-специално в областта на безопасността на продуктите, киберсигурността, конкуренцията, цифровите и медийните услуги, финансовите услуги, защитата на потребителите, защитата на данните и на основните права;
 - и) да допринася за ефективното сътрудничество с компетентните органи на трети държави и с международни организации;
 - й) да подпомага националните компетентни органи и Комисията при развиването на организационния и техническия експертен опит, необходим за прилагането на настоящия регламент, включително като допринася за оценката на нуждите от обучение на персонала на държавите членки, участващ в прилагането на настоящия регламент;
 - к) да съдейства на Службата по ИИ при подпомагането на националните компетентни органи за създаването и разработването на регулаторни лаборатории в областта на ИИ и да улеснява сътрудничеството и обмена на информация между регулаторните лаборатории в областта на ИИ;
 - л) да допринася и предоставя съответни консултации при разработването на документи с насоки;
 - м) да консултира Комисията по международни въпроси, свързани с ИИ;
 - н) да предоставя становища на Комисията относно приоритетните сигнали във връзка с модели на ИИ с общо предназначение;
 - о) да получава становища от държавите членки относно приоритетните сигнали относно моделите на ИИ с общо предназначение и относно националния опит и практики във връзка с мониторинга и осигуряването на спазването във връзка със системите с ИИ, по-специално системите, интегриращи модели на ИИ с общо предназначение.

Член 67

Консултативен форум

1. Създава се консултативен форум, който да осигурява технически експертен опит и да консултира Съвета по ИИ и Комисията, както и да допринася за изпълнението на техните задачи съгласно настоящия регламент.
2. Членовете на консултативния форум представляват балансирано подбрани представители на заинтересовани страни, сред които стопанския сектор, новосъздадените предприятия, МСП, гражданското общество и академичните среди. Осигурява се баланс сред членовете на консултативния форум по отношение на търговските и нетърговските интереси, а в рамките на категорията на търговските интереси – по отношение на МСП и други предприятия.
3. Комисията избира членовете на консултативния форум в съответствие с критериите, посочени в параграф 2, сред заинтересованите страни с признат експертен опит в областта на ИИ.

4. Мандатът на членовете на консултативния форум е с продължителност от две години, като може да бъде удължен до не повече от четири години.
5. Агенцията за основните права, ENISA, Европейският комитет по стандартизация (CEN), Европейският комитет за стандартизация в електротехниката (CENELEC) и Европейският институт за стандарти в далекосъобщенията (ETSI) са постоянни членове на Консултативния форум.
6. Консултативният съвет изготвя свой процедурен правилник. Той избира двама съпредседатели измежду своите членове в съответствие с критериите, посочени в параграф 2. Мандатът на съпредседателите е две години с право на еднократно подновяване.
7. Консултативният форум провежда заседания най-малко два пъти годишно. Консултативният форум може да кани експерти и други заинтересовани страни на своите заседания.
8. Консултативният форум може да изготвя мнения, препоръки и писмени становища при поискване от Съвета по ИИ или от Комисията.
9. Консултативният форум може да създава постоянни или временни подгрупи, когато това е целесъобразно за разглеждането на конкретни въпроси, свързани с целите на настоящия регламент.
10. Консултативният форум изготвя ежегоден доклад за своите дейности. Този доклад е обществено достъпен.

Член 68

Експертна група, съставена от независими експерти

1. Комисията приема чрез акт за изпълнение разпоредби относно създаването на експертна група, съставена от независими експерти (наричана по-долу „експертната група“), предназначена да подпомага дейностите по осигуряване на спазването на настоящия регламент. Този акт за изпълнение се приема в съответствие с процедурата по разглеждане, посочена в член 98, параграф 2.
2. Експертната група се състои от експерти, избрани от Комисията въз основа на съвременни научни или технически експертни познания в областта на изкуствения интелект, необходими за изпълнението на задачите, посочени в параграф 3, и трябва да е в състояние да докаже, че отговаря на всички посочени по-долу условия:
 - а) наличие на специфичен експертен опит и компетентност и научен или технически експертен опит в областта на ИИ;
 - б) независимост от доставчици на системи с ИИ или модели на ИИ с общо предназначение;
 - в) способност за надлежно, точно и обективно извършване на дейностите.Комисията, като се консултира със Съвета по ИИ, определя броя на експертите в групата в съответствие с потребностите и гарантира справедливо представителство на половете и географско представителство.
3. Експертната група консултира и подпомага Службата по ИИ, по-специално по отношение на следните задачи:
 - а) подпомагане на прилагането и осигуряване на спазването на настоящия регламент по отношение на моделите и системите с ИИ с общо предназначение, по-специално чрез
 - i) предупреждаване на Службата за ИИ за възможни системни рискове на равнището на Съюза за моделите на ИИ с общо предназначение в съответствие с член 90;
 - ii) принос за разработването на инструменти и методологии за оценка на способностите на моделите и системите с ИИ с общо предназначение, включително чрез сравнителни показатели;
 - iii) консултации относно класифицирането на моделите на ИИ с общо предназначение, пораждащи системен риск;
 - iv) консултации относно различните модели и системи с ИИ с общо предназначение;

- в) принос за разработването на инструменти и образци;
- б) подпомагане на работата на органите за надзор на пазара по тяхно искане;
- в) подпомагане на трансграничните дейности по надзор на пазара, посочени в член 74, параграф 11, без да се засягат правомощията на органите за надзор на пазара;
- г) подпомагане на Службата по ИИ при изпълнението на нейните задължения в контекста на предпазната процедура на Съюза съгласно член 81.

4. Експертите от експертната група изпълняват задачите си безпристрастно и обективно и гарантират поверителността на информацията и данните, получени при изпълнението на техните задачи и дейности. Те не търсят, нито приемат указания от никого при изпълнение на задачите си по параграф 3. Всеки експерт попълва декларация за интереси, която се оповестява публично. Службата по ИИ установява системи и процедури за активно управление и предотвратяване на потенциални конфликти на интереси.

5. Актът за изпълнение, посочен в параграф 1, включва разпоредби относно условията, процедурите и подробните правила, въз основа на които експертната група и нейните членове да подават сигнали и да искат съдействие от Службата за ИИ за изпълнението на задачите на експертната група.

Член 69

Достъп на държавите членки до резерва от експерти

1. Държавите членки могат да се обърнат към експерти от експертната група, за да ги подпомогнат в техните дейности по осигуряване на спазването на настоящия регламент.
2. От държавите членки може да се изисква заплащането на такси за предоставените от експертите консултации и подкрепа. Структурата и размерът на таксите, както и размерът и структурата на подлежащите на възстановяване разходи се определят в акта за изпълнение, посочен в член 68, параграф 1, като се вземат предвид целите за адекватно прилагане на настоящия регламент и разходна ефективност, както и необходимостта да се осигури ефективен достъп до експерти от всички държави членки.
3. Комисията улеснява навременния достъп на държавите членки до експертите, когато е необходимо, и гарантира, че комбинирането на дейностите за подкрепа, осъществявани от структурите на Съюза за подкрепа на изпитванията в областта на ИИ съгласно член 84 и от експерти съгласно настоящия член, е организирано по ефикасен начин и осигурява възможно най-висока добавена стойност.

РАЗДЕЛ 2

Национални компетентни органи

Член 70

Определяне на национални компетентни органи и единно звено за контакт

1. Всяка държава членка създава или определя като национални компетентни органи най-малко един нотифициращ орган и най-малко един орган за надзор на пазара за целите на настоящия регламент. Тези национални компетентни органи упражняват правомощията си независимо, безпристрастно и непредубедено, за да бъде спазена обективността в дейностите и задачите им и да се гарантира прилагането и изпълнението на настоящия регламент. Членовете на тези органи се въздържат от всякакво действие, несъвместимо с техните функции. При спазване на посочените принципи, дейностите и задачите могат да се изпълняват от един или повече определени органи в съответствие с организационните нужди на държавата членка.
2. Държавите членки съобщават на Комисията идентификационните данни на нотифициращите органи и органите за надзор на пазара и задачите на тези органи, както и всички последващи промени във връзка с тях. Държавите членки оповестяват публично информацията за това как може да се осъществи връзка с компетентните органи и единните звена за контакт чрез електронни средства за комуникация до 2 август 2025 г. Държавите членки определят орган за надзор на пазара, който да действа като единно звено за контакт за настоящия регламент, и съобщават на Комисията идентификационните данни на единното звено за контакт. Комисията осигурява публично достъпен списък на определените единни звена за контакт.

3. Държавите членки гарантират, че техните национални компетентни органи разполагат с достатъчно технически, финансови и човешки ресурси и с инфраструктура, за да изпълняват ефективно задачите си съгласно настоящия регламент. По-специално националните компетентни органи трябва да разполагат с достатъчен брой постоянно наличен персонал, чиято компетентност и експертен опит включват задълбочено разбиране на технологиите за ИИ, данните и компютърните системи за данни, защитата на личните данни, киберсигурността, основните права, рисковете за здравето и безопасността, както и познаване на съществуващите стандарти и правни изисквания. Държавите членки ежегодно оценяват и при необходимост актуализират изискванията за компетентност и ресурси, посочени в настоящия параграф.
4. Националните компетентни органи вземат подходящи мерки за осигуряване на адекватно ниво на киберсигурност.
5. При изпълнение на своите задачи националните компетентни органи действат в съответствие със задълженията за поверителност, установени в член 78.
6. До 2 август 2025 г. и веднъж на всеки две години след това държавите членки докладват на Комисията за състоянието на финансовите и човешките ресурси, с които разполагат националните компетентни органи, с оценка на тяхната адекватност. Комисията предава тази информация на Съвета по ИИ за обсъждане и евентуални препоръки.
7. Комисията улеснява обмена на опит между националните компетентни органи.
8. Националните компетентни органи могат да предоставят насоки и съвети относно прилагането на настоящия регламент, по-специално на МСП, включително новосъздадените предприятия, като отчитат насоките и консултациите със Съвета по ИИ и Комисията, в зависимост от случая. Когато националните компетентни органи възнамеряват да дадат насоки и консултации във връзка със система с ИИ в области, обхванати от друго право на Съюза, когато е целесъобразно, се провеждат консултации с националните компетентни органи съгласно посоченото право на Съюза.
9. Когато институциите, органите, службите или агенциите на Съюза попадат в обхвата на настоящия регламент, Европейският надзорен орган по защита на данните действа като компетентен орган за техния надзор.

ГЛАВА VIII

БАЗА ДАННИ НА ЕС ЗА ВИСОКОРИСКОВИ СИСТЕМИ С ИИ

Член 71

База данни на ЕС за високорисковите системи с ИИ, изброени в приложение III

1. Комисията, в сътрудничество с държавите членки, създава и поддържа база данни на ЕС, съдържаща посочената в параграфи 2 и 3 от настоящия член информация относно високорисковите системи с ИИ, посочени в член 6, параграф 2, които са регистрирани в съответствие с членове 49 и 60, и системи с ИИ, които не се считат за високорискови съгласно член 6, параграф 3 и които са регистрирани в съответствие с член 6, параграф 4 и член 49. При определянето на функционалните спецификации на такава база данни Комисията се консултира със съответните експерти, а при актуализирането на функционалните спецификации на тази база данни Комисията се консултира със Съвета по ИИ.
2. Данните, изброени в раздели А и Б от приложение VIII се въвеждат в базата данни на ЕС от доставчика или, в зависимост от случая, от упълномощения представител.
3. Данните, изброени в раздел В от приложение VIII, се въвеждат в базата данни на ЕС от внедрителя, който е или действа от името на публичен орган, агенция или структура в съответствие с член 49, параграфи 3 и 4.
4. С изключение на раздела, посочен в член 49, параграф 4 и член 60, параграф 4, буква в), информацията, съдържаща се в базата данни на ЕС, регистрирана в съответствие с член 49, е достъпна и публично достъпна по лесен за използване начин. Информацията следва да бъде лесна за навигация и машинно четима. Информацията, регистрирана в съответствие с член 60, е достъпна само за органите за надзор на пазара и Комисията, освен ако потенциалният доставчик или доставчикът не е дал съгласието си тази информация да бъде достъпна и за обществеността.
5. 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 законно право да представляват доставчика или внедрителя, в зависимост от случая.

6. Комисията е администратор на базата данни на ЕС. Тя предоставя на доставчиците, потенциалните доставчици и внедрителите подходяща техническа и административна подкрепа. Базата данни трябва да отговаря на приложимите изисквания за достъпност.

ГЛАВА IX

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

РАЗДЕЛ 1

Мониторинг след пускането на пазара

Член 72

Мониторинг, извършван 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, които могат да бъдат предоставени от внедрителите или да бъдат събрани чрез други източници относно функционирането на високорисковите системи с ИИ през целия им жизнен цикъл, и които позволяват на доставчика да оценява непрекъснатото съответствие на системите с ИИ с изискванията, установени в глава III, раздел 2. Когато е целесъобразно, мониторингът след пускането на пазара включва анализ на взаимодействието с други системи с ИИ. Това задължение не обхваща чувствителни оперативни данни на внедрители, които са правоохранителни органи.
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. До 2 февруари 2026 г. Комисията приема акт за изпълнение за установяване на подробни разпоредби за утвърждаване на образец на плана за мониторинг след пускането на пазара и списък на елементите, които трябва да бъдат включени в плана. Този акт за изпълнение се приема в съответствие с процедурата по разглеждане, посочена в член 98, параграф 2.
4. За да се гарантира съгласуваност, да се избегне дублиране и да се сведе до минимум допълнителната тежест, по отношение на високорисковите системи с ИИ, обхванати от законодателството на Съюза за хармонизация, посочено в раздел A от приложение I, когато съгласно това законодателство вече е създадена система и план за мониторинг след пускането на пазара, доставчиците могат да изберат да интегрират, когато е целесъобразно, необходимите елементи, описани в параграфи 1, 2 и 3, като използват образца, посочен в параграф 3, във вече съществуващи системи и планове съгласно посоченото законодателство, при условие че се постига равностойно равнище на защита.

Първа алинея от настоящия параграф се прилага и за високорисковите системи с ИИ, посочени в точка 5 от приложение III, които са пуснати на пазара или пуснати в действие от финансови институции, спрямо които съгласно правото на Съюза в областта на финансовите услуги се прилагат изисквания по отношение на тяхното вътрешно управление, мерки или процеси.

РАЗДЕЛ 2

Обмен на информация за сериозни инциденти

Член 73

Докладване на сериозни инциденти

1. Доставчиците на високорискови системи с ИИ, пуснати на пазара на Съюза, докладват за всеки сериозен инцидент на органите за надзор на пазара на държавите членки, в които е възникнал инцидентът.

2. Докладът, посочен в параграф 1, се изготвя незабавно, след като доставчикът установи причинно-следствена връзка между системата с ИИ и сериозния инцидент или правдоподобна вероятност за такава връзка и във всеки случай не по-късно от 15 дни след като доставчикът или, когато е приложимо, внедрителят, научи за сериозния инцидент.

Срокът за докладването, посочено в първа алинея, е съобразен с тежестта на сериозния инцидент.

3. Независимо от параграф 2 от настоящия член, в случай на широко разпространено нарушение или сериозен инцидент съгласно определението в член 3, точка 49, буква б), докладът, посочен в параграф 1 от настоящия член, се представя незабавно и не по-късно от два дни, след като доставчикът или, когато е приложимо, внедрителят научи за инцидента.

4. Независимо от параграф 2, в случай на смърт на лице, докладът се представя незабавно след като доставчикът или внедрителят установи или веднага щом предположи наличието на причинно-следствена връзка между високорисковата система с ИИ и сериозния инцидент, но не по-късно от 10 дни след датата, на която доставчикът или, когато е приложимо, внедрителят научи за сериозния инцидент.

5. Когато е необходимо да се гарантира своевременно докладване, доставчикът или, когато е приложимо, внедрителят може да представи непълен първоначален доклад, последван от пълен доклад.

6. След докладването на сериозен инцидент съгласно параграф 1 доставчикът незабавно провежда необходимите разследвания във връзка със сериозния инцидент и съответната система с ИИ. Това включва оценка на риска, свързан с инцидента, и коригиращи действия.

По време на разследванията, посочени в първа алинея, доставчикът си сътрудничи с компетентните органи и, когато е целесъобразно, със съответния нотифициран орган и не провежда разследвания, включващи промяна на съответната система с ИИ по начин, който може да засегне всяка последваща оценка на причините за инцидента, преди да информира компетентните органи за това действие.

7. При получаване на уведомление, свързано със сериозен инцидент съгласно член 3, точка 49, буква в), съответният орган за надзор на пазара информира националните публични органи или структури, посочени в член 77, параграф 1. Комисията разработва специални насоки за улесняване на спазването на задълженията, посочени в параграф 1 от настоящия член. Тези насоки се изготвят до 2 август 2025 г. и подлежат на редовна оценка.

8. Органът за надзор на пазара предприема подходящи мерки съгласно член 19 от Регламент (ЕС) 2019/1020 в срок от седем дни от датата на получаване на уведомлението, посочено в параграф 1 от настоящия член, и прилага процедурите за уведомяване, предвидени в посочения регламент.

9. За високорисковите системи с ИИ, посочени в приложение III, които са пуснати на пазара или пуснати в действие от доставчици, за които се прилагат законодателни актове на Съюза, в които се предвиждат задължения за докладване, равностойни на установените в настоящия регламент, уведомяването за сериозни инциденти се ограничава до посочените в член 3, точка 49, буква в) сериозни инциденти.

10. За високорисковите системи с ИИ, които са защитни елементи на устройства или сами по себе си са устройства, попадащи в обхвата на регламенти (ЕС) 2017/745 и (ЕС) 2017/746, уведомлението за сериозни инциденти се ограничава до посочените в член 3, точка 49, буква в) от настоящия регламент сериозни инциденти и се отправя до националния компетентен орган, избран за тази цел от държавите членки, в които е възникнал инцидентът.

11. Националните компетентни органи незабавно уведомяват Комисията за всеки сериозен инцидент, независимо от това дали са предприели действия по него, в съответствие с член 20 от Регламент (ЕС) 2019/1020.

РАЗДЕЛ 3

Осигуряване на спазването

Член 74

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 осигуряване на спазването на настоящия регламент:

- а) всяко позоваване на икономически оператор съгласно Регламент (ЕС) 2019/1020 се разбира като включващо всички оператори, посочени в член 2, параграф 1 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. Като част от задълженията си за докладване съгласно член 34, параграф 4 от Регламент (ЕС) 2019/1020 органите за надзор на пазара докладват ежегодно 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. Те също така докладват ежегодно на Комисията за използването на забранени практики през същата година и за предприетите мерки.

3. За високорисковите системи с ИИ, свързани с продукти, за които се прилага законодателството на Съюза, посочено в раздел А от приложение I, органът за надзор на пазара за целите на настоящия регламент е органът, отговарящ за дейностите по надзор на пазара, определен съгласно съответните правни актове.

Чрез дерогация от първа алинея и при подходящи обстоятелства държавите членки могат да определят друг съответен орган, който да действа като орган за надзор на пазара, при условие че е осигурена координация със съответните секторни органи за надзор на пазара, отговарящи за осигуряването на спазването на законодателството на Съюза за хармонизация, посочено в приложение I.

4. Процедурите, посочени в членове 79—83 от настоящия регламент, не се прилагат за системи с ИИ, свързани с продукти, за които се прилага законодателството на Съюза за хармонизация, посочено в раздел А от приложение I, когато в посочените правни актове вече са предвидени процедури, които гарантират равностойно равнище на защита и които имат същата цел. В тези случаи вместо това се прилагат съответните секторни процедури.

5. Без да се засягат правомощията на органите за надзор на пазара съгласно член 14 от Регламент (ЕС) 2019/1020, с цел да се гарантира ефективното осигуряване на спазването на настоящия регламент, органите за надзор на пазара могат, когато е целесъобразно, да упражняват от разстояние правомощията, посочени в член 14, параграф 4, буква г) и й) от посочения регламент.

6. За високорисковите системи с ИИ, пуснати на пазара, пуснати в действие или използвани от финансови институции, регулирани от правото на Съюза в областта на финансовите услуги, органът за надзор на пазара за целите на настоящия регламент е съответният национален орган, отговарящ за финансовия надзор на тези институции съгласно посоченото законодателство, доколкото пускането на пазара, пускането в действие или използването на системата с ИИ е пряко свързано с предоставянето на тези финансови услуги.

7. Чрез дерогация от параграф 6, при подходящи обстоятелства и при условие че е осигурена координация, държавата членка може да определи друг съответен орган за орган за надзор на пазара за целите на настоящия регламент.

Националните органи за надзор на пазара, упражняващи надзор върху кредитни институции, регулирани съгласно Директива 2013/36/ЕС, които участват в единния надзорен механизъм, създаден с Регламент (ЕС) № 1024/2013, следва незабавно да докладват на Европейската централна банка всяка информация, установена в хода на дейностите им по надзор на пазара, която може да представлява потенциален интерес във връзка със задачите на Европейската централна банка по упражняване на пруденциален надзор, предвидени в посочения регламент.

8. За високорисковите системи с ИИ, изброени в точка 1 от приложение III към настоящия регламент, доколкото системите се използват за правоохранителни цели, управление на границите и правосъдие и демокрация, както и за високорисковите системи с ИИ, изброени в точки 6, 7 и 8 от приложение III към настоящия регламент, държавите членки определят органи за надзор на пазара за целите на настоящия регламент или компетентните надзорни органи за защита на данните съгласно Регламент (ЕС) 2016/679 или Директива (ЕС) 2016/680, или всеки друг орган, определен съгласно същите условия, предвидени в членове 41 – 44 от Директива (ЕС) 2016/680. Дейностите по надзор на пазара по никакъв начин не засягат независимостта на съдебните органи, нито засягат по друг начин тяхната дейност при изпълнение на съдебните им функции.

9. Когато институциите, органите, службите или агенциите на Съюза попадат в обхвата на настоящия регламент, Европейският надзорен орган по защита на данните действа като техен орган за надзор на пазара, освен по отношение на Съда на Европейския съюз при изпълнение на съдебните му функции.

10. 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 I, или друго право на Съюза, което може да е от значение за високорисковите системи с ИИ, посочени в приложение III.

11. Органите за надзор на пазара и Комисията могат да предлагат съвместни дейности, включително съвместни разследвания, които да се провеждат или от органите за надзор на пазара, или от органите за надзор на пазара съвместно с Комисията, и да имат за цел насърчаване на постигането на съответствие, установяване на несъответствие, повишаване на осведомеността или даването на насоки във връзка с настоящия регламент по отношение на конкретни категории високорискови системи с ИИ, за които е установено, че представляват сериозен риск в две или повече държави членки в съответствие с член 9 от Регламент (ЕС) 2019/1020. Службата по ИИ осигурява централна координация на съвместното разследване.

12. Без да се засягат правомощията, предвидени в Регламент (ЕС) 2019/1020, и когато е приложимо, в рамките на необходимото за изпълнение на задачите им, органите за надзор на пазара получават от доставчиците пълен достъп до документацията и до наборите от обучителни, валидационни и изпитвателни данни, използвани за разработването на високорискови системи с ИИ, включително, когато е целесъобразно и при наличие на гаранции за сигурността, чрез приложно-програмни интерфейси (API) или други подходящи технически средства и инструменти, позволяващи дистанционен достъп.

13. На органите за надзор на пазара се предоставя достъп до изходния код на високорисковата система с ИИ при отправено обосновано искане и само ако са изпълнени двете посочени по-долу условия:

- a) достъпът до изходния код е необходим, за да се оцени съответствието на високорисковата система с ИИ с изискванията, установени в глава III, раздел 2; и
- b) процедурите за изпитване или одит и проверките въз основа на данните и документацията, предоставени от доставчика, са изчерпани или са се оказали недостатъчни.

14. Всяка информация или документация, получена от органите за надзор на пазара, се третира в съответствие със задълженията за поверителност, установени в член 78.

Член 75

Взаимопомощ, надзор на пазара и контрол на системите с ИИ с общо предназначение

1. Когато дадена система с ИИ се основава на модел на ИИ с общо предназначение и моделът и системата са разработени от един и същ доставчик, Службата по ИИ има правомощия да наблюдава и упражнява надзор за съответствието на тази система с ИИ от гледна точка на задълженията по настоящия регламент. За да изпълнява задачите си по мониторинг и надзор, Службата по ИИ разполага с всички правомощия на орган за надзор на пазара, предвидени в настоящия раздел и в Регламент (ЕС) 2019/1020.

2. Когато съответните органи за надзор на пазара имат достатъчно основания да считат, че системите с ИИ с общо предназначение, които могат да се използват пряко от внедрителите за най-малко една цел, която е класифицирана като високорискова съгласно настоящия регламент, не съответстват на изискванията, установени в настоящия регламент, те си сътрудничат със Службата по ИИ, за да извършват оценки на съответствието и съответно информират Съвета по ИИ и другите органи за надзор на пазара.

3. Когато органът за надзор на пазара не е в състояние да приключи своето разследване на високорисковата система с ИИ поради невъзможността да получи достъп до определена информация, свързана с модела на ИИ с общо предназначение, въпреки че е положил всички необходими усилия, за да получи тази информация, той може да подаде обосновано искане до Службата по ИИ, в която се осигурява достъп до тази информация. В този случай Службата по ИИ предоставя на органа заявител -без забавяне и при всички случаи в срок от 30 дни - всяка информация, която Службата по ИИ счита за целесъобразна, за да се установи дали дадена високорискова система с ИИ не съответства на изискванията. Органите за надзор на пазара гарантират поверителността на информацията, която получават в съответствие с член 78 от настоящия регламент. Процедурата, предвидена в глава VI от Регламент (ЕС) 2019/1020, се прилага *mutatis mutandis*.

Член 76

Надзор върху изпитването в реални условия, упражняван от органите за надзор на пазара

1. Органите за надзор на пазара разполагат с компетентността и правомощията да гарантират, че изпитването в реални условия е в съответствие с настоящия регламент.

2. Когато се извършва изпитване в реални условия на системи с ИИ, върху които се упражнява надзор в регулаторна лаборатория в областта на ИИ съгласно член 58, органите за надзор на пазара проверяват съответствието с член 60 като част от надзорната си функция по отношение на регулаторната лаборатория в областта на ИИ. Тези органи могат, когато е целесъобразно, да разрешат изпитването в реални условия да се извършва от доставчика или потенциалния доставчик чрез дерогация от условията, установени в член 60, параграф 4, букви е) и ж).

3. Когато орган за надзор на пазара е бил информиран за сериозен инцидент от потенциален доставчик, доставчик или трето лице или има други основания да счита, че условията по членове 60 и 61 не са изпълнени, той може да вземе някое от следните решения на своята територия, в зависимост от случая:

а) да спре или да прекрати изпитването в реални условия;

б) да изиска от доставчика или потенциалния доставчик и внедрителя или потенциалния внедрител да променят който и да е аспект на изпитването в реални условия.

4. Когато орган за надзор на пазара е взел решение, посочено в параграф 3 от настоящия член, или е отправил възражение по смисъла на член 60, параграф 4, буква б), в решението или възражението се посочват основанията за него и редът и условията, при които доставчикът или потенциалният доставчик може да оспори решението или възражението.

5. Когато е приложимо, ако орган за надзор на пазара е взел решение, посочено в параграф 3, той съобщава основанията за това решение на органите за надзор на пазара на другите държави членки, в които системата с ИИ е била изпитвана в съответствие с плана за изпитване.

Член 77

Правомощия на органите за защита на основните права

1. Националните публични органи или структури, които упражняват надзор или осигуряват спазването на задълженията съгласно правото на Съюза за защита на основните права, включително правото на недискриминация, във връзка с използването на високорисковите системи с ИИ, посочени в приложение III, имат правомощието да изискват и получават достъп до всякаква документация, създадена или поддържана съгласно настоящия регламент на достъпен език и формат, когато достъпът до тази документация е необходим за ефективното упражняване на правомощията им в рамките на тяхната юрисдикция. Съответният публичен орган или структура информира органа за надзор на пазара на съответната държава членка за всяко такова искане.

2. До 2 ноември 2024 г. всяка държава членка определя публичните органи или структури, посочени в параграф 1, и оповестява публично списъка на тези органи. Държавите членки уведомяват Комисията и другите държави членки за списъка и го актуализират редовно.

3. Когато документацията, посочена в параграф 1, е недостатъчна, за да се установи дали е извършено нарушение на задълженията съгласно правото на Съюза за защита на основните права, публичният орган или структура по параграф 1 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 отправилния искането публичен орган или структура в разумен срок след подаване на искането.

4. Всяка информация или документация, получени съгласно настоящия член от националните публични органи или структури, посочени в параграф 1 от настоящия член, се третира в съответствие със задълженията за поверителност, установени в член 78.

Член 78

Поверителност

1. Комисията, органите за надзор на пазара и нотифицираните органи, както и други физически или юридически лица, участващи в прилагането на настоящия регламент, в съответствие с правото на Съюза или националното право, защитат 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 (ЕС) 2016/943 на Европейския парламент и на Съвета⁽⁵⁷⁾;
- б) ефективното прилагане на настоящия регламент, по-специално за целите на проверките, разследванията или одитите;
- в) обществените интереси и интересите на националната сигурност;
- г) провеждането на наказателни или административни производства;
- д) информацията, класифицирана съгласно правото на Съюза или националното право.

2. Органите, участващи в прилагането на настоящия регламент съгласно параграф 1, изискват само данни, които са строго необходими за оценката на риска, породен от системите с ИИ, и за упражняването на техните правомощия в съответствие с настоящия регламент и с Регламент (ЕС) 2019/1020. Те въвеждат подходящи и ефективни мерки за киберсигурност за защита на сигурността и поверителността на получената информация и данни и в съответствие с приложимото право на Съюза или национално право заличават събраните данни веднага след като те престанат да са необходими за целта, за която са били получени.

3. Без да се засягат параграфи 1 и 2, 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 тази информация, и с внедрителя, когато високорисковите системи с ИИ, посочени в точка 1, 6 или 7 от приложение III, се използват от правоохранителните органи, органите за граничен контрол, имиграционните органи или органите в областта на убежището, и когато такова разкриване би застрашило обществените интереси и интересите на националната сигурност. Този обмен на информация не обхваща чувствителни оперативни данни във връзка с дейностите на правоохранителните органи, органите за граничен контрол, имиграционните органи или органите в областта на убежището.

Когато правоохранителните органи, имиграционните органи или органите в областта на убежището са доставчици на високорисковите системи с ИИ, посочени в точка 1, 6 или 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 74, параграфи 8 и 9, зависимост от 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, преминал съответното проучване за надеждност.

4. Параграфи 1, 2 и 3 не засягат правата или задълженията на Комисията, държавите членки и съответните им органи, както и тези на нотифицираните органи по отношение на обмена на информация и разпространяването на предупреждения, включително в контекста на трансграничното сътрудничество, нито засягат задълженията на съответните лица за предоставяне на информация съгласно наказателното право на държавите членки.

5. Комисията и държавите членки могат - при необходимост и в съответствие със съответните разпоредби на международни и търговски споразумения - да обменят поверителна информация с регулаторните органи на трети държави, с които са сключили двустранни или многостранни споразумения за поверителност, гарантиращи адекватно равнище на поверителност.

Член 79

Процедура на национално равнище, приложима за системи с ИИ, представляващи риск

1. Системите с ИИ, представляващи риск, се считат за продукт, представляващ риск, съгласно определението в член 3, точка 19 от Регламент (ЕС) 2019/1020, доколкото те представляват рискове за здравето или безопасността или за 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 съгласно параграф 1 от настоящия член, той извършва оценяване на съответната система с ИИ по отношение на нейното съответствие с всички изисквания и задължения, установени в настоящия регламент. Особено внимание се обръща на системите с ИИ, представляващи риск за уязвими групи. Когато бъдат установени рискове за основните права, органът за надзор на пазара също така информира и изцяло сътрудничи със съответните национални публични органи или структури, посочени в член 77, параграф 1. Съответните оператори сътрудничат при необходимост с органа за надзор на пазара и с другите национални публични органи или структури, посочени в член 77, параграф 1.

⁽⁵⁷⁾ Директива (ЕС) 2016/943 на Европейския парламент и на Съвета от 8 юни 2016 г. относно защитата на неразкрити ноу-хау и търговска информация (търговски тайни) срещу тяхното незаконно придобиване, използване и разкриване (ОВ L 157, 15.6.2016 г., стр. 1).

Когато в хода на това оценяване органът за надзор на пазара или, когато е приложимо, органът за надзор на пазара - в сътрудничество с националния публичен орган по член 77, параграф 1 - констатира, че системата с ИИ не съответства на изискванията и задълженията, установени в настоящия регламент, той без ненужно забавяне изисква от съответния оператор да предприеме всички подходящи коригиращи действия, за да приведе в съответствие системата с ИИ, да я изтегли от пазара или да я изведе в разумен срок, определен от органа за надзор на пазара, и във всички случаи не по-късно от 15 работни дни, или съгласно съответното право на Съюза за хармонизация.

Органът за надзор на пазара надлежно информира съответния нотифициран орган. Спрямо мерки, посочени във втора алинея от настоящия параграф, 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 без ненужно забавяне Комисията и другите държави членки за резултатите от оценяването и за действията, които е изискал да бъдат предприети от оператора.

4. Операторът гарантира предприемането на всички подходящи коригиращи действия по отношение на всички засегнати системи с ИИ, които е предоставил на пазара на Съюза.

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 подходящи временни мерки, за да забрани или ограничи предоставянето на системата с ИИ на пазара на съответната държава членка или пусната в действие, за да изтегли продукта или самостоятелната система с ИИ от пазара, или за да ги изведе. Този орган уведомява без ненужно забавяне Комисията и другите държави членки за тези мерки.

6. Уведомлението по параграф 5 включва всички налични подробни данни, по-специално информацията, необходима за идентифицирането на несъответстващата система с ИИ, произхода на системата с ИИ и веригата на доставка, 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) нарушение на забраната на практиките в областта на ИИ, посочени в член 5;
- б) несъответствие на високорисковата система с ИИ с изискванията, установени в глава III, раздел 2;
- в) недостатъци в хармонизираните стандарти или в общите спецификации, посочени в членове 40 и 41, на които се основава презумпцията за съответствие;
- г) нарушение на член 50.

7. Органите за надзор на пазара, различни от органа за надзор на пазара на държавата членка, започнала процедурата, без ненужно забавяне информират Комисията и другите държави членки за всички приети мерки и за всяка допълнителна информация, с която разполагат във връзка с 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 уведомлението, посочено в параграф 5 от настоящия член, не е повдигнато възражение от орган за надзор на пазара на държава членка или от Комисията във връзка с временна мярка, предприета от орган за надзор на пазара на друга 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. Тримесечният срок, посочен в настоящия параграф, се намалява на 30 дни в случай на нарушение на забраната на практиките в областта на ИИ, посочени в член 5 от настоящия регламент.

9. Органите за надзор на пазара гарантират предприемането без ненужно забавяне на подходящи ограничителни мерки по отношение на продукта или системата с ИИ, като например изтеглянето на продукта или системата с ИИ от пазара им.

Член 80

Процедура за работа със системи с ИИ, класифицирани от доставчика като непредставляващи високорискови при прилагане на приложение III

1. Когато орган за надзор на пазара има достатъчно основания да счита, че дадена система с ИИ, класифицирана от доставчика като непредставляваща високорискова съгласно член 6, параграф 3, в действителност е високорискова, органът за надзор на пазара извършва оценка на съответната система с ИИ по отношение на класифицирането ѝ като високорискова система с ИИ въз основа на условията, посочени в член 6, параграф 3 и насоките на Комисията.

2. Когато в хода на тази оценка органът за надзор на пазара установи, че съответната система с ИИ е високорискова, той без ненужно забавяне изисква от съответния доставчик да предприеме всички необходими действия, за да приведе системата с ИИ в съответствие с изискванията и задълженията, установени в настоящия регламент, както и да предприеме подходящи коригиращи действия в срока, определен от органа за надзор на пазара.
3. Когато органът за надзор на пазара счита, че използването на съответната система с ИИ не е ограничено само до националната му територия, той информира без ненужно забавяне Комисията и другите държави членки за резултатите от оценяването и за действията, които е изискал да бъдат предприети от доставчика.
4. Доставчикът гарантира, че са предприети всички необходими действия за привеждане на системата с ИИ в съответствие с изискванията и задълженията, установени в настоящия регламент. Когато доставчикът на система с ИИ не приведе системата с ИИ в съответствие с тези изисквания и задължения в рамките на срока, посочен в параграф 2 от настоящия член, на доставчика се налагат глоби и имуществени санкции в съответствие с член 99.
5. Доставчикът осигурява предприемането на подходящи коригиращи действия по отношение на всички съответни системи с ИИ, които е предоставил на пазара на Съюза.
6. Когато доставчикът на съответната система с ИИ не предприеме подходящи коригиращи действия в срока, посочен в параграф 2 от настоящия член, се прилага член 79, параграфи 5 – 9.
7. Когато в хода на оценката съгласно параграф 1 от настоящия член органът за надзор на пазара установи, че системата с ИИ е била неправилно класифицирана от доставчика като не представляваща високорискова, за да се заобиколи прилагането на изискванията в глава III, раздел 2, на доставчика се налагат глоби и имуществени санкции в съответствие с член 99.
8. При упражняване на правомощието си за мониторинг на прилагането на настоящия член и в съответствие с член 11 от Регламент (ЕС) 2019/1020 органите за надзор на пазара могат да извършват подходящи проверки, като вземат предвид по-специално информацията, съхранявана в базата данни на ЕС, посочена в член 71 от настоящия регламент.

Член 81

Предпазна процедура на Съюза

1. Когато в срок от три месеца след получаване на уведомлението по член 79, параграф 5 или в срок от 30 дни, в случай на нарушение на забраната на практиките в областта на ИИ, посочени в член 5, органът за надзор на пазара на държава членка е повдигнал възражения срещу мярка, предприета от друг орган за надзор на пазара, или когато Комисията счита, че мярката противоречи на правото на Съюза, Комисията незабавно започва консултации с органа за надзор на пазара на съответната държава членка и със 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 в срок от шест месеца или в срок от 60 дни в случай на нарушение на забраната на практики в областта на ИИ, посочени в член 5, като срокът започва да тече от уведомлението, посочено в член 79, параграф 5, и съобщава решението си на органа за надзор на пазара на съответната държава членка. Комисията информира за своето решение и всички други органи за надзор на пазара.
2. Когато Комисията счете, че мярката, предприета от съответната държава членка е оправдана, всички държави членки гарантират, че предприемат подходящи ограничителни мерки по отношение на съответната система с ИИ, например изискване за изтеглянето на системата с ИИ от техния пазар без ненужно забавяне, и уведомяват Комисията за това. Когато Комисията счете, че националната мярка не е оправдана, съответната държава членка отменя мярката и уведомява Комисията за това.
3. Когато бъде преценено, че националната мярка е оправдана 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 82

Съответстващи на изискванията системи с ИИ, които представляват риск

1. Когато орган за надзор на пазара на държава членка, след като извърши оценката съгласно член 79, след консултация със съответния национален публичен орган, посочен в член 77, параграф 1, установи, че макар дадена високорискова система с ИИ да е в съответствие с настоящия регламент, тя представлява риск за здравето или безопасността на хората, за 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 системата с ИИ бъде пусната на пазара или пусната в действие, тя няма да представлява такъв риск, без ненужно забавяне в срок, определен от органа.

2. Доставчикът или друг съответен оператор гарантира предприемането на коригиращи действия по отношение на всички съответни системи с ИИ, които е предоставил на пазара на Съюза, в рамките на срока, определен от органа за надзор на пазара на държавата членка, посочен в параграф 1.
3. Държавите членки незабавно информират Комисията и другите държави членки за констатацията съгласно параграф 1. 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 започва без ненужно забавяне консултации със съответните държави членки и съответните оператори и оценява предприетите национални мерки. Въз основа на резултатите от тази оценка Комисията взема решение дали мярката е оправдана и когато е необходимо, предлага други подходящи мерки.
5. Комисията незабавно съобщава решението си на съответните държави членки и съответните оператори. Тя информира за него и другите държави членки.

Член 83

Формално несъответствие

1. Когато органът за надзор на пазара на дадена държава членка направи някоя от следните констатации, той изисква от съответния доставчик да прекрати несъответствието в срок, определен от органа за надзор на пазара:
 - а) маркировката „СЕ“ е нанесена в нарушение на член 48;
 - б) маркировката „СЕ“ не е нанесена;
 - в) ЕС декларацията за съответствие, посочена в член 47, не е съставена;
 - г) ЕС декларацията за съответствие, посочена в член 47, е съставена неправилно;
 - д) регистрацията в базата данни на ЕС, посочена в член 71, не е извършена;
 - е) когато е приложимо, не е определен упълномощен представител;
 - ж) техническата документация не е налична.

2. Когато несъответствието, посочено в параграф 1, продължи, органът за надзор на пазара на съответната държава членка предприема подходящи и пропорционални мерки, за да ограничи или да забрани предоставянето на високорисковата система с ИИ на пазара или да осигури нейното изтегляне или изземване от пазара без забавяне.

Член 84

Структури на Съюза за подкрепа на изпитванията в областта на ИИ

1. Комисията определя една или повече структури на Съюза за подкрепа на изпитванията в областта на ИИ за изпълнение на задачите, изброени съгласно член 21, параграф 6 от Регламент (ЕС) 2019/1020 в областта на ИИ.
2. Без да се засягат задачите, посочени в параграф 1, структурите на Съюза за подкрепа на изпитванията в областта на ИИ предоставят и независими технически или научни консултации по искане на Съвета по ИИ, Комисията или органите за надзор на пазара.

РАЗДЕЛ 4

Средства за защита

Член 85

Право на подаване на жалба до орган за надзор на пазара

Без да се засягат другите административни или съдебни средства за защита, всяко физическо или юридическо лице, което има основания да счита, че е налице нарушение на настоящия регламент, може да подаде жалби до съответния орган за надзор на пазара.

В съответствие с Регламент (ЕС) 2019/1020 тези жалби се вземат предвид за целите на провеждането на дейности по надзор на пазара и се разглеждат в съответствие със специалните процедури, установени за тази цел от органите за надзор на пазара.

Член 86

Право на обяснение при вземане на индивидуални решения

1. Всяко засегнато лице, което е обект на решение, взето от внедрителя въз основа на резултатите от високорискова система с ИИ, посочена в приложение III, с изключение на системите, изброени в точка 2 от посоченото приложение, и което поражда правни последици или по подобен начин значително засяга това лице така, че то да счита, че се оказва неблагоприятно въздействие върху неговото здраве, безопасност или основни права, има право да получи от внедрителя ясни и съдържателни обяснения за мястото на системата с ИИ в процедурата за вземане на решения и основните елементи на взетото решение.

2. Параграф 1 не се прилага за използването на системи с ИИ, за които изключенията или ограниченията на задължението по посочения параграф произтичат от правото на Съюза или националното право, съвместимо с правото на Съюза.

3. Настоящият член се прилага само доколкото правото, посочено в параграф 1, не е предвидено по друг начин в правото на Съюза.

Член 87

Сигнали за нарушения и защита на подаващите сигнали лица

По отношение на подаването на сигнали за нарушения по настоящия регламент и защитата на лицата, подаващи сигнали за такива нарушения, се прилага Директива (ЕС) 2019/1937.

РАЗДЕЛ 5

Надзор, разследване, осигуряване на спазването и мониторинг по отношение на доставчиците на модели на ИИ с общо предназначение

Член 88

Изпълнение на задълженията на доставчиците на модели на ИИ с общо предназначение

1. Комисията разполага с изключителни правомощия за надзор и осигуряване на спазването на глава V, като взема предвид процедурните гаранции по член 94. Комисията възлага изпълнението на тези задачи на Службата по ИИ, без да се засягат организационните правомощия на Комисията и разделението на областите на компетентност между държавите членки и Съюза въз основа на Договорите.

2. Без да се засяга член 75, параграф 3, органите за надзор на пазара могат да поискат от Комисията да упражни правомощията, предвидени в настоящия раздел, когато това е необходимо и пропорционално за подпомагане на изпълнението на техните задачи съгласно настоящия регламент.

Член 89

Действия по мониторинг

1. За целите на изпълнението на задачите, възложени ѝ съгласно настоящия раздел, Службата по ИИ може да предприеме необходимите дейности по мониторинг на ефективното изпълнение и осигуряване на спазването на настоящия регламент от страна на доставчиците на модели на ИИ с общо предназначение, включително придържането от тяхна страна към одобрени кодекси за добри практики.
2. Доставчиците надолу по веригата имат право да подадат жалба с твърдения за нарушение на настоящия регламент. Жалбата трябва да е надлежно мотивирана и да съдържа най-малко информация за:
 - а) звеното за контакт на доставчика на съответния модел на ИИ с общо предназначение;
 - б) описание на съответните факти, съответните разпоредби на настоящия регламент и основанията, поради които доставчикът надолу по веригата счита, че доставчикът на съответния модел на ИИ с общо предназначение е нарушил настоящия регламент;
 - в) всяка друга информация, която доставчикът надолу по веригата, изпратил искането, счита за относима, включително, когато е подходящо, информация, събрана по негова собствена инициатива.

Член 90

Сигнали за системни рискове от експертната група

1. Експертната група може да изпрати приоритетен сигнал до Службата по ИИ, когато има основания да предполага, че:
 - а) модел на ИИ с общо предназначение поражда конкретен установим риск на равнището на Съюза; или
 - б) модел на ИИ с общо предназначение съответства на условията, посочени в член 51.
2. При получаване на такъв приоритетен сигнал Комисията, чрез Службата по ИИ и след като е информирала Съвета по ИИ, може да упражни правомощията, предвидени в настоящия раздел, с цел преценка на въпроса. Службата по ИИ информира Съвета по ИИ за всяка мярка съгласно членове 91—94.
3. Приоритетният сигнал трябва да е надлежно мотивиран и да съдържа най-малко информация за:
 - а) звеното за контакт на доставчика на съответния модел на ИИ с общо предназначение, пораждащ системен риск;
 - б) описание на съответните факти и причините за сигнала от експертната група;
 - в) всяка друга информация, която експертната група счита за относима, включително, ако е подходящо, информация, събрана по нейна собствена инициатива.

Член 91

Правомощия за изискване на документация и информация

1. Комисията може да поиска от доставчика на съответния модел на ИИ с общо предназначение да предостави документацията, изготвена от доставчика в съответствие с членове 53 и 55, или всякаква допълнителна информация, която е необходима за целите на оценката на съответствието на доставчика с настоящия регламент.
2. Преди да изпрати искането за информация, Службата по ИИ може да започне структуриран диалог с доставчика на модела на ИИ с общо предназначение.
3. При надлежно обосновано искане от експертната група Комисията може да отправи искане за предоставяне на информация до доставчик на модел на ИИ с общо предназначение, когато достъпът до информация е необходим и пропорционален за изпълнението на задачите на експертната група съгласно член 68, параграф 2.

4. В искането за информация се посочват правното основание и целта на искането, конкретизира се каква информация се изисква, определя се срок, в който информацията трябва да бъде предоставена, и се посочват глобите, предвидени в член 101 за предоставяне на неточна, непълна или подвеждаща информация.

5. Доставчикът на съответния модел на ИИ с общо предназначение или негов представител предоставят исканата информация. В случай на юридически лица, дружества или предприятия, или когато доставчикът няма правосубектност, лицата, упълномощени да ги представляват по закон или съгласно учредителните им документи, предоставят исканата информация от името на доставчика на съответния модел на ИИ с общо предназначение. Надлежно упълномощени адвокати могат да предоставят информация от името на своите клиенти. Въпреки това клиентите остават изцяло отговорни, ако предоставената информация е непълна, неточна или подвеждаща.

Член 92

Правомощия за извършване на оценки

1. Службата по ИИ, след консултация със Съвета по ИИ, може да извършва оценки на съответния модел на ИИ с общо предназначение с цел:

- a) оценяване на спазването от страна на доставчика на задълженията по настоящия регламент, когато събраната съгласно член 91 информация е недостатъчна; или
- b) проучване на системните рискове на равнището на Съюза на моделите на ИИ с общо предназначение, поражащи системен риск, по-специално след приоритетен сигнал от експертната група в съответствие с член 90, параграф 1, буква а).

2. Комисията може да реши да назначи независими експерти, които да извършват оценки от нейно име, включително от експертната група, създадена съгласно член 68. Независимите експерти, назначени за тази задача, трябва да отговарят на критериите, посочени в член 68, параграф 2.

3. За целите на параграф 1 Комисията може да поиска достъп до съответния модел на ИИ с общо предназначение чрез API или други подходящи технически средства и инструменти, включително изходен код.

4. В искането за достъп се посочват правното основание, целта и мотивите на искането, както и срокът за предоставяне на достъп, както и глобите, предвидени в член 101, ако не бъде предоставен достъп.

5. Доставчиците на съответния модел на ИИ с общо предназначение или техният представител представят поисканата информация. В случаите на юридически лица, дружества или предприятия, или когато доставчикът няма правосубектност – лицата, упълномощени да ги представляват по закон или съгласно учредителните им документи, осигуряват поискания достъп от името на доставчика на съответния модел на ИИ с общо предназначение.

6. Комисията приема актове за изпълнение, в които се установяват подробните правила и условията за извършването на оценките, включително подробните правила за участието на независими експерти, както и процедурата за техния подбор. Тези актове за изпълнение се приемат в съответствие с процедурата по разглеждане, посочена в член 98, параграф 2.

7. Преди да поиска достъп до съответния модел на ИИ с общо предназначение, Службата по ИИ може да започне структуриран диалог с доставчика на модела на ИИ с общо предназначение, за да събере повече информация относно вътрешното изпитване на модела, вътрешните гаранции за предотвратяване на системни рискове и други вътрешни процедури и мерки, които доставчикът е предприел за смекчаване на тези рискове.

Член 93

Правомощие за отправяне на искания за предприемане на мерки

1. Когато е необходимо и целесъобразно, Комисията може да поиска от доставчиците:

- a) да предприемат подходящи мерки за спазване на задълженията, установени в членове 53 и 54;

- б) да прилагат мерки за смекчаване на риска, когато оценката, извършена в съответствие с член 92, е породила сериозно и основателно опасение за системен риск на равнището на Съюза;
- в) да ограничат предоставянето на пазара, да изтеглят или да изземат модела.

2. Преди отправяне на искането за предприемане на мярка Службата по ИИ може да започне структуриран диалог с доставчика на модела на ИИ с общо предназначение.

3. Ако по време на структурирания диалог, посочен в параграф 2, доставчикът на модела на ИИ с общо предназначение, пораждащ системен риск, предложи поемането на ангажменти за прилагане на мерки за смекчаване на риска с цел справяне със системни рискове на равнището на Съюза, Комисията може с решение да придаде на тези ангажменти задължителен характер и да посочи, че няма допълнителни основания за действие.

Член 94

Процедурни права на икономическите оператори на модела на ИИ с общо предназначение

Член 18 от Регламент (ЕС) 2019/1020 се прилага *mutatis mutandis* за доставчиците на модела на ИИ с общо предназначение, без да се засягат специалните процедурни права, предвидени в настоящия регламент.

ГЛАВА X

КОДЕКСИ ЗА ПОВЕДЕНИЕ И НАСОКИ

Член 95

Кодекси за поведение за прилагане на специфични изисквания на доброволна основа

1. Службата по ИИ и държавите членки насърчават и улесняват изготвянето на кодекси за поведение, включително свързаните с тях механизми за управление, предназначени да насърчават прилагането на доброволна основа към системи с ИИ, различни от високорискови системи с ИИ, на някои или всички изисквания, установени в глава III, раздел 2, като вземат предвид наличните технически решения и най-добрите практики в сектора, които позволяват прилагането на такива изисквания.

2. Службата по ИИ и държавите членки улесняват изготвянето на кодекси за поведение относно прилагането на доброволна основа, включително от страна на внедрителите, на специфични изисквания по отношение на всички системи с ИИ, въз основа на ясни цели и ключови показатели за ефективност с цел оценяване на постигането на тези цели, включително елементи като, но не само:

- а) приложими елементи, предвидени в етичните насоки на Съюза за надежден ИИ;
- б) оценяване и свеждане до минимум на въздействието на системите с ИИ върху екологичната устойчивост, включително по отношение на ефективното от енергийна гледна точка програмиране и техниките за ефективно проектиране, обучение и използване на ИИ;
- в) насърчаване на грамотността в областта на ИИ, по-специално на лицата, които се занимават с разработването, функционирането и използването на ИИ;
- г) улесняване на приобщаващото и разнообразно проектиране на системите с ИИ, включително чрез създаването на приобщаващи екипи от разработчици, които се характеризират и с разнообразие, и насърчаване на участието на заинтересованите страни в този процес;
- д) оценяване и предотвратяване на отрицателното въздействие на системите с ИИ върху уязвимите лица или групи уязвими лица, включително по отношение на достъпността за лица с увреждания, както и върху равенството между половете.

3. Кодексите за поведение могат да бъдат изготвяни от отделни доставчици или внедрители на системи с ИИ или от организации, които ги представляват, или съвместно, включително с участието на всички заинтересовани страни и техните представителни организации, включително организации на гражданското общество и академичните среди. Кодексите за поведение могат да обхващат една или повече системи с ИИ, като се отчита сходството в предназначението на съответните системи.

4. При насърчаването и улесняването на изготвянето на кодекси за поведение Службата по ИИ и държавите членки вземат предвид особените интереси и нужди на МСП, включително новосъздадените предприятия.

Член 96

Насоки от Комисията относно прилагането на настоящия регламент

1. Комисията разработва насоки относно практическото прилагане на настоящия регламент, и по-специално относно:
 - а) прилагането на изискванията и задълженията, посочени в членове 8—15 и в член 25;
 - б) забранените практики, посочени в член 5;
 - в) практическото прилагане на разпоредбите, свързани със съществени изменения;
 - г) практическото изпълнение на задълженията за прозрачност, предвидени в член 50;
 - д) подробна информация относно връзката на настоящия регламент със законодателството на Съюза за хармонизация, посочено в приложение I, както и с друго приложимо право на Съюза, включително по отношение на съгласуваността при осигуряване на спазването им;
 - е) прилагането на определението за система с ИИ, посочено в член 3, точка 1.

Когато отправя на такива насоки, Комисията обръща специално внимание на нуждите на МСП, включително новосъздадените предприятия, на органите на местна власт и на секторите, които е най-вероятно да бъдат засегнати от настоящия регламент.

Насоките, посочени в първа алинея от настоящия параграф, трябва да са надлежно съобразени с общопризнатите съвременни технически постижения в областта на ИИ, както и със съответните хармонизирани стандарти и общи спецификации, посочени в членове 40 и 41, или с хармонизираните стандарти или техническите спецификации, които са установени съгласно правото на Съюза за хармонизация.

2. По искане на държавите членки или на Службата по ИИ, или по собствена инициатива Комисията актуализира вече приетите насоки, когато счете това за необходимо.

ГЛАВА XI

ДЕЛЕГИРАНЕ НА ПРАВОМОЩИЯ И ПРОЦЕДУРА НА КОМИТЕТ

Член 97

Упражняване на делегирането

1. Правомощието да приема делегирани актове се предоставя на Комисията при спазване на предвидените в настоящия член условия.
2. Правомощието да приема делегирани актове, посочено в член 6, параграфи 6 и 7, член 7, параграфи 1 и 3, член 11, параграф 3, член 43, параграфи 5 и 6, член 47, параграф 5, член 51, параграф 3, член 52, параграф 4 и член 53, параграфи 5 и 6, се предоставя на Комисията за срок от пет години, считано от 1 август 2024 г. Комисията изготвя доклад относно делегирането на правомощия не по-късно от девет месеца преди изтичането на петгодишния срок. Делегирането на правомощия се продължава мълчаливо за срокове с еднаква продължителност, освен ако Европейският парламент или Съветът не възразят срещу подобно продължаване не по-късно от три месеца преди изтичането на всеки срок.
3. Делегирането на правомощия, посочено в член 6, параграфи 6 и 7, член 7, параграфи 1 и 3, член 11, параграф 3, член 43, параграфи 5 и 6, член 47, параграф 5, член 51, параграф 3, член 52, параграф 4 и член 53, параграфи 5 и 6, 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 публикуването му в *Официален вестник на Европейския съюз* или на по-късна, посочена в решението дата. То не засяга действителността на делегираните актове, които вече са в сила.
4. Преди приемането на делегиран акт Комисията се консултира с експерти, определени от всяка държава членка в съответствие с принципите, залегнали в Междунституционалното споразумение от 13 април 2016 г. за по-добро законотворчество.

5. Веднага след като приеме делегиран акт, Комисията нотифицира акта едновременно на Европейския парламент и на Съвета.

6. Делегиран акт, приет съгласно член 6, параграф 6 или 7, член 7, параграф 1 или 3, член 11, параграф 3, член 43, параграф 5 или 6, член 47, параграф 5, член 51, параграф 3, член 52, параграф 4 или член 53, параграф 5 или 6, 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 98

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.

ГЛАВА XII

САНКЦИИ

Член 99

Санкции

1. В съответствие с реда и условията, предвидени в настоящия регламент, държавите членки установяват система от санкции и други принудителни мерки, които могат да включват и предупреждения и неимуществени мерки, приложими при нарушения на настоящия регламент от операторите, и вземат всички необходими мерки, за да гарантират, че те се прилагат правилно и ефективно, като при това вземат предвид насоките, отправени от Комисията съгласно член 96. Предвидените санкции трябва да бъдат ефективни, пропорционални и възпиращи. Те трябва да бъдат съобразени с интересите на МСП, включително новосъздадените предприятия, и тяхната икономическа жизнеспособност.

2. Държавите членки, незабавно и най-късно до началната дата на прилагане, уведомяват Комисията за правилата относно санкциите и другите принудителни мерки, посочени в параграф 1, и я уведомяват незабавно за всяко последващо изменение в тях.

3. Нарушението на забраната на практиките в областта на ИИ, посочени в член 5, се наказва с административни глоби и имуществени санкции в размер до 35 000 000 EUR или, ако нарушителят е предприятие, до 7 % от общия му годишен световен оборот за предходната финансова година, като се прилага по-големият размер.

4. Нарушението на някоя от посочените по-долу разпоредби, свързани с операторите или нотифицираните органи, различни от посочените в член 5, се наказва с административни глоби и имуществени санкции в размер до 15 000 000 EUR или, ако нарушителят е предприятие, до 3 % от общия му годишен световен оборот за предходната финансова година, като се прилага по-големият размер:

- а) задължения на доставчиците съгласно член 16;
- б) задължения на упълномощените представители съгласно член 22;
- в) задължения на вносителите съгласно член 23;
- г) задължения на дистрибуторите съгласно член 24;
- д) задължения на внедрителите съгласно член 26;
- е) изисквания и задължения на нотифицираните органи съгласно член 31, член 33, параграфи 1, 3 и 4 или член 34;
- ж) задължения за прозрачност на доставчиците и внедрителите съгласно член 50.

5. Предоставянето на неточна, непълна или подвеждаща информация в отговор на искане от нотифицираните органи или националните компетентни органи се наказва с административни глоби и имуществени санкции в размер до 7 500 000 EUR или, ако нарушителят е предприятие, до 1 % от общия му годишен световен оборот за предходната финансова година, като се прилага по-големият размер.
6. В случая на МСП, включително новосъздадени предприятия, всяка глоба или имуществена санкция, посочена в настоящия член, е в размер до процентите или сумата, посочени в параграфи 3, 5 и 4, като се прилага по-ниският размер.
7. При вземането на решение дали да бъде наложена административна глоба или имуществена санкция и относно размера на административната глоба или имуществена санкция във всеки отделен случай се вземат предвид всички обстоятелства от значение за конкретния случай и, доколкото е приложимо, се обръща надлежно внимание на следното:
- а) естеството, тежестта и продължителността на нарушението и последиците от него, като се вземат предвид целта на системата с ИИ, както и когато е приложимо, броят на засегнатите лица и степента на причинената им вреда;
 - б) дали други органи за надзор на пазара вече са наложили административни глоби или имуществени санкции на същия оператор за същото нарушение;
 - в) дали други органи вече са наложили административни глоби или имуществени санкции на същия оператор за нарушения на друго право на Съюза или национално право, когато тези нарушения са резултат от същата дейност или бездействие, съставляващи съответно нарушение на настоящия регламент;
 - г) размера, годишния оборот и пазарния дял на оператора, извършил нарушението;
 - д) всякакви други утежняващи или смекчаващи обстоятелства, приложими към обстоятелствата по случая, като пряко или косвено реализирани имуществени ползи или избегнати загуби вследствие на нарушението;
 - е) степента на сътрудничество с националните компетентни органи с цел прекратяване на нарушението и ограничаване на евентуалните неблагоприятни последици от него;
 - ж) степента на отговорност на оператора, като се вземат предвид техническите и организационните мерки, прилагани от него;
 - з) начина, по който нарушението е станало известно на националните компетентни органи, по-специално дали операторът е уведомил за нарушението и ако го е направил, в каква степен;
 - и) дали нарушението е извършено умишлено, или по небрежност;
 - й) всички действия, предприети от оператора за намаляване на вредите, претърпени от засегнатите лица.
8. Всяка държава членка определя правила за това до каква степен могат да бъдат налагани административни имуществени санкции на публични органи и структури, установени в тази държава членка.
9. В зависимост от правната система на държавите членки правилата относно административните глоби и имуществени санкции могат да се прилагат по такъв начин, че санкциите да се налагат от компетентните национални съдилища или други органи според практиката в тези държави членки. Прилагането на тези правила в тези държави членки трябва да има равностоен ефект.
10. Упражняването на правомощията по настоящия член зависи от съответните процедурни гаранции в съответствие с правото на Съюза и националното право, включително ефективни правни средства за защита и справедлив съдебен процес.
11. Държавите членки ежегодно докладват на Комисията за административните глоби и имуществени санкции, които са наложили през същата година в съответствие с настоящия член, както и за всички свързани съдебни спорове или съдебни производства.

Член 100

Административни глоби, налагани на институциите, органите, службите и агенциите на Съюза

1. Европейският надзорен орган по защита на данните може да налага административни глоби на институциите, органите, службите и агенциите на Съюза, попадащи в обхвата на настоящия регламент. При вземането на решение дали да бъде наложена административна глоба и 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, като се вземат предвид целта на съответната система с ИИ, както и, когато е приложимо, броят на засегнатите лица и степента на претърпените от тях вреди;
- б) степента на отговорност на институцията, органа, службата или агенцията на Съюза, като се вземат предвид техническите и организационните мерки, прилагани от тях;
- в) всички действия, предприети от институцията, органа, службата или агенцията на Съюза за намаляване на претърпяната от засегнатите лица вреда;
- г) степента на сътрудничеството с Европейския надзорен орган по защита на данните с цел прекратяване на нарушението и ограничаване на евентуалните неблагоприятни последици от него, включително спазването на всяка от мерките, разпоредени преди това от Европейския надзорен орган по защита на данните срещу съответната институция, орган, служба или агенция на Съюза по същия въпрос;
- д) всички подобни предходни нарушения от страна на институция, орган, служба или агенция на Съюза;
- е) начинът, по който нарушението е станало известно на Европейския надзорен орган по защита на данните, по-специално дали и до каква степен институцията, органа, службата или агенцията на Съюза са съобщили за нарушението;
- ж) годишния бюджет на институцията, органа, службата или агенцията на Съюза.

2. Нарушението на забраната на практиките с ИИ, посочени в член 5, се наказва с административни глоби в размер до 1 500 000 EUR.

3. Несъответствието на системата с ИИ с изисквания или задължения по настоящия регламент, различни от посочените в член 5, се наказва с административни глоби в размер до 750 000 EUR.

4. Преди да вземе решение съгласно настоящия член, Европейският надзорен орган по защита на данните дава на институцията, органа, службата или агенцията на Съюза, по отношение на които се провежда производството 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 елементи и обстоятелства, по които засегнатите страни са имали възможност да изразят становище. Евентуалните жалбоподатели 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 глоби съгласно настоящия член, се използват за общия бюджет на Съюза. Глобите не трябва да засягат ефективното функциониране на санкционираната институция, орган, служба или агенция на Съюза.

7. Европейският надзорен орган по защита на данните ежегодно уведомява Комисията за административните глоби, които е наложил съгласно настоящия член, и за всички съдебни спорове или съдебни производства, които е започнал.

Член 101

Глоби за доставчиците на модели на ИИ с общо предназначение

1. Комисията може да наложи на доставчиците на модели с ИИ с общо предназначение глоби, които не надвишават 3 % от общия им годишен световен оборот през предходната финансова година или 15 000 000 EUR, като се прилага по-високият размер, когато Комисията установи, че доставчикът умишлено или поради небрежност:

- а) е нарушил съответните разпоредби на настоящия регламент;
- б) не е изпълнил изискване за предоставяне на документация или информация съгласно член 91 или е предоставил неточна, непълна или подвеждаща информация;
- в) не е изпълнил мярка, поискана съгласно член 93;

- г) не е предоставил на Комисията достъп до модела на ИИ с общо предназначение или модела на ИИ с общо предназначение, пораждащ системен риск, с оглед на извършването на оценка съгласно член 92.

При определяне на размера на глобата или периодичната имуществена санкция се вземат предвид естеството, тежестта и продължителността на нарушението, като се отчитат надлежно принципите на пропорционалност и целесъобразност. Комисията също така взема предвид ангажиментите, поети в съответствие с член 93, параграф 3 или закрепени в съответните кодекси за добри практики в съответствие с член 56.

2. Преди да приеме решението съгласно параграф 1, Комисията съобщава предварителните си констатации на доставчика на модела на ИИ с общо предназначение и му дава възможност да бъде изслушан.
3. Глобите, налагани в съответствие с настоящия член, трябва да са ефективни, пропорционални и възпиращи.
4. Информацията относно глобите, наложени съгласно настоящия член, се съобщава и на Съвета по ИИ, когато е целесъобразно.
5. Съдът на Европейския съюз разполага с неограничена компетентност за контрол върху решенията на Комисията, с които се налага глоба съгласно настоящия член. Той може да отмени, да намали или да увеличи наложената глоба.
6. Комисията приема актове за изпълнение, съдържащи подробни правила и процедурни гаранции във връзка с процедурите с оглед на евентуалното приемане на решения съгласно параграф 1 от настоящия член. Тези актове за изпълнение се приемат в съответствие с процедурата по разглеждане, посочена в член 98, параграф 2.

ГЛАВА XIII

ЗАКЛЮЧИТЕЛНИ РАЗПОРЕДБИ

Член 102

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) 2024/1689 на Европейския парламент и на Съвета (*), се вземат предвид изискванията, установени в глава III, раздел 2 от посочения регламент.

(*) Регламент (ЕС) 2024/1689 на Европейския парламент и на Съвета от 13 юни 2024 г. за установяване на хармонизирани правила относно изкуствения интелект и за изменение на регламенти (ЕО) № 300/2008, (ЕС) № 167/2013, (ЕС) № 168/2013, (ЕС) 2018/858, (ЕС) 2018/1139 и (ЕС) 2019/2144 и директиви 2014/90/ЕС, (ЕС) 2016/797 и (ЕС) 2020/1828 (Акт за изкуствения интелект) (ОВ L, 2024/1689, 12.7.2024 г., ELI: <https://eur-lex.europa.eu/eli/reg/2024/1689/oj>).“

Член 103

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) 2024/1689 на Европейския парламент и на Съвета (*), се вземат предвид изискванията, установени в глава III, раздел 2 от посочения регламент.

(*) Регламент (ЕС) 2024/1689 на Европейския парламент и на Съвета от 13 юни 2024 г. за установяване на хармонизирани правила относно изкуствения интелект и за изменение на регламенти (ЕО) № 300/2008, (ЕС) № 167/2013, (ЕС) № 168/2013, (ЕС) 2018/858, (ЕС) 2018/1139 и (ЕС) 2019/2144 и директиви 2014/90/ЕС, (ЕС) 2016/797 и (ЕС) 2020/1828 (Акт за изкуствения интелект) (ОВ L, 2024/1689, 12.7.2024 г., ELI: <https://eur-lex.europa.eu/eli/reg/2024/1689/oj>).“

Член 104

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) 2024/1689 на Европейския парламент и на Съвета (*), се вземат предвид изискванията, установени в глава III, раздел 2 от посочения регламент.

(*) Регламент (ЕС) 2024/1689 на Европейския парламент и на Съвета от 13 юни 2024 г. за установяване на хармонизирани правила относно изкуствения интелект и за изменение на регламенти (ЕО) № 300/2008, (ЕС) № 167/2013, (ЕС) № 168/2013, (ЕС) 2018/858, (ЕС) 2018/1139 и (ЕС) 2019/2144 и директиви 2014/90/ЕС, (ЕС) 2016/797 и (ЕС) 2020/1828 (Акт за изкуствения интелект) (ОВ L, 2024/1689, 12.7.2024 г., ELI: <https://eur-lex.europa.eu/eli/reg/2024/1689/oj>).“

Член 105

Изменение на Директива 2014/90/ЕС

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

„5. За системите с изкуствен интелект, които представляват защитни елементи по смисъла на Регламент (ЕС) 2024/1689 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, установени в глава III, раздел 2 от посочения регламент.

(*) Регламент (ЕС) 2024/1689 на Европейския парламент и на Съвета от 13 юни 2024 г. за установяване на хармонизирани правила относно изкуствения интелект и за изменение на регламенти (ЕО) № 300/2008, (ЕС) № 167/2013, (ЕС) № 168/2013, (ЕС) 2018/858, (ЕС) 2018/1139 и (ЕС) 2019/2144 и директиви 2014/90/ЕС, (ЕС) 2016/797 и (ЕС) 2020/1828 (Акт за изкуствения интелект) (ОВ L, 2024/1689, 12.7.2024 г., ELI: <https://eur-lex.europa.eu/eli/reg/2024/1689/oj>).“

Член 106

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) 2024/1689 на Европейския парламент и на Съвета (*), се вземат предвид изискванията, установени в глава III, раздел 2 от посочения регламент.

(*) Регламент (ЕС) 2024/1689 на Европейския парламент и на Съвета от 13 юни 2024 г. за установяване на хармонизирани правила относно изкуствения интелект и за изменение на регламенти (ЕО) № 300/2008, (ЕС) № 167/2013, (ЕС) № 168/2013, (ЕС) 2018/858, (ЕС) 2018/1139 и (ЕС) 2019/2144 и директиви 2014/90/ЕС, (ЕС) 2016/797 и (ЕС) 2020/1828 (Акт за изкуствения интелект) (ОВ L, 2024/1689, 12.7.2024 г., ELI: <https://eur-lex.europa.eu/eli/reg/2024/1689/oj>).“

Член 107

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) 2024/1689 на Европейския парламент и на Съвета (*), се вземат предвид изискванията, установени в глава III, раздел 2 от посочения регламент.

(*) Регламент (ЕС) 2024/1689 на Европейския парламент и на Съвета от 13 юни 2024 г. за установяване на хармонизирани правила относно изкуствения интелект и за изменение на регламенти (ЕО) № 300/2008, (ЕС) № 167/2013, (ЕС) № 168/2013, (ЕС) 2018/858, (ЕС) 2018/1139 и (ЕС) 2019/2144 и директиви 2014/90/ЕС, (ЕС) 2016/797 и (ЕС) 2020/1828 (Акт за изкуствения интелект) (ОВ L, 2024/1689, 12.7.2024 г., ELI: <https://eur-lex.europa.eu/eli/reg/2024/1689/oj>).“

Член 108

Изменения 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) 2024/1689 на Европейския парламент и на Съвета (*), се вземат предвид изискванията, установени в глава III, раздел 2 от посочения регламент.

(*) Регламент (ЕС) 2024/1689 на Европейския парламент и на Съвета от 13 юни 2024 г. за установяване на хармонизирани правила относно изкуствения интелект и за изменение на регламенти (ЕО) № 300/2008, (ЕС) № 167/2013, (ЕС) № 168/2013, (ЕС) 2018/858, (ЕС) 2018/1139 и (ЕС) 2019/2144 и директиви 2014/90/ЕС, (ЕС) 2016/797 и (ЕС) 2020/1828 (Акт за изкуствения интелект) (ОВ L, 2024/1689, 12.7.2024 г., ELI: <https://eur-lex.europa.eu/eli/reg/2024/1689/oj>).“

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) 2024/1689, се вземат предвид изискванията, установени в глава III, раздел 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) 2024/1689, се вземат предвид изискванията, установени в глава III, раздел 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) 2024/1689, се вземат предвид изискванията, установени в глава III, раздел 2 от посочения регламент.“

5) В член 57 се добавя следната алинея:

„При приемането на тези актове за изпълнение относно системи с изкуствен интелект, които представляват защитни елементи по смисъла на Регламент (ЕС) 2024/1689, се вземат предвид изискванията, установени в глава III, раздел 2 от посочения регламент.“

б) 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) 2024/1689, се вземат предвид изискванията, установени в глава III, раздел 2 от посочения регламент.“.

Член 109

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) 2024/1689 на Европейския парламент и на Съвета (*), се вземат предвид изискванията, установени в глава III, раздел 2 от посочения регламент.

(*) Регламент (ЕС) 2024/1689 на Европейския парламент и на Съвета от 13 юни 2024 г. за установяване на хармонизирани правила относно изкуствения интелект и за изменение на регламенти (ЕО) № 300/2008, (ЕС) № 167/2013, (ЕС) № 168/2013, (ЕС) 2018/858, (ЕС) 2018/1139 и (ЕС) 2019/2144 и директиви 2014/90/ЕС, (ЕС) 2016/797 и (ЕС) 2020/1828 (Акт за изкуствения интелект) (ОВ L, 2024/1689, 12.7.2024 г., ELI: <http://data.europa.eu/eli/reg/2024/1689/oj>).“

Член 110

Изменение на Директива (ЕС) 2020/1828

В приложение I към Директива (ЕС) 2020/1828 на Европейския парламент и на Съвета ⁽⁵⁸⁾ се добавя следната точка:

„68) Регламент (ЕС) 2024/1689 на Европейския парламент и на Съвета от 13 юни 2024 г. за установяване на хармонизирани правила относно изкуствения интелект и за изменение на регламенти (ЕО) № 300/2008, (ЕС) № 167/2013, (ЕС) № 168/2013, (ЕС) 2018/858, (ЕС) 2018/1139 и (ЕС) 2019/2144 и директиви 2014/90/ЕС, (ЕС) 2016/797 и (ЕС) 2020/1828 (Акт за изкуствения интелект) (ОВ L, 2024/1689, 12.7.2024 г., ELI: <http://data.europa.eu/eli/reg/2024/1689/oj>).“

Член 111

Системи с ИИ, които вече са пуснати на пазара или пуснати в действие, и модели на ИИ с общо предназначение, които вече са пуснати на пазара

1. Без да се засяга прилагането на член 5 съгласно посоченото в член 113, параграф 3, буква а), системите с ИИ, които са компоненти на широкомащабните информационни системи, създадени с правните актове, изброени в приложение X, които са пуснати на пазара или пуснати в действие преди 2 август 2027 г., се привеждат в съответствие с настоящия регламент до 31 декември 2030 г.

Изискванията, установени в настоящия регламент, се вземат предвид при оценката на всяка широкомащабна информационна система, създадена с правните актове, изброени в приложение X, която трябва да бъде предприета съгласно предвиденото в тези правни актове, както и когато тези правни актове се заменят или изменят.

2. Без да се засяга прилагането на член 5 съгласно член 113, параграф 3, буква а), настоящият регламент се прилага по отношение на операторите на високорискови системи с ИИ, различни от системите, посочени в параграф 1 от настоящия член, които са пуснати на пазара или пуснати в действие преди 2 август 2026 г., само ако от посочената дата тези системи претърпяват значителни изменения в проекта си. При всички случаи доставчиците и внедрителите на високорискови системи с ИИ, предназначени да бъдат използвани от публичните органи, предприемат необходимите мерки с цел постигане на съответствие с изискванията и задълженията по настоящия регламент до 2 август 2030 г.

3. Доставчиците на модели на ИИ с общо предназначение, които са били пуснати на пазара преди 2 август 2025 г. предприемат необходимите мерки с цел изпълнение на задълженията, предвидени в настоящия регламент, до 2 август 2027 г.

⁽⁵⁸⁾ Директива (ЕС) 2020/1828 на Европейския парламент и на Съвета от 25 ноември 2020 г. относно представителни искове за защита на колективните интереси на потребителите и за отмяна на Директива 2009/22/ЕО (ОВ L 409, 4.12.2020 г., стр. 1).

Член 112

Оценка и преглед

1. Комисията оценява необходимостта от изменение на списъка в приложение III и списъка на забранените практики в областта на ИИ в член 5 веднъж годишно след влизането в сила на настоящия регламент и до края на срока на делегирането на правомощията, посочен в член 97. Комисията представя констатациите от тази оценка на Европейския парламент и на Съвета.
2. До 2 август 2028 г. и на всеки четири години след това Комисията оценява и представя на Европейския парламент и на Съвета доклад относно следното:
 - а) необходимостта от изменение с цел разширяване на съществуващите функции по области или за добавяне на нови функции по области в приложение III;
 - б) изменение на списъка на системите с ИИ, за които се изискват допълнителни мерки за прозрачност съгласно член 50;
 - в) изменение с цел повишаване на ефективността на системата за надзор и управление.
3. До 2 август 2029 г. и на всеки четири години след това Комисията представя на Европейския парламент и на Съвета доклад относно оценката и прегледа на настоящия регламент. Докладът включва оценка по отношение на структурата на осигуряването на спазването на настоящия регламент и евентуалната необходимост от създаването на агенция на Съюза с цел отстраняване на установените недостатъци. Въз основа на констатациите докладът се придружава, когато е целесъобразно, от предложение за изменение на настоящия регламент. Тези доклади се оповестяват публично.
4. В докладите, посочени в параграф 2, се отделя специално внимание на следното:
 - а) състоянието на финансовите, техническите и човешките ресурси на националните компетентни органи с оглед на ефективното изпълнение на задачите, които са им възложени съгласно настоящия регламент;
 - б) санкциите, по-специално административните глоби и имуществени санкции, посочени в член 99, параграф 1, налагани от държавите членки за нарушения на настоящия регламент;
 - в) приетите хармонизирани стандарти и общи спецификации, разработени за подпомагане на прилагането на настоящия регламент;
 - г) броя на предприятията, които навлизат на пазара след влизането в сила на настоящия регламент, и колко от тях са МСП.
5. До 2 август 2028 г. Комисията извършва оценка на функционирането на Службата по ИИ, преценява дали на Службата по ИИ са предоставени достатъчно правомощия и компетентност, за да изпълнява задачите си, и дали за правилното изпълнение и прилагане на настоящия регламент би било целесъобразно и необходимо да се усъвършенства Службата по ИИ и нейната компетентност в областта на осигуряване на спазването, както и да се увеличат нейните ресурси. Комисията представя доклад относно оценката си на Европейския парламент и на Съвета.
6. До 2 август 2028 г. и на всеки четири години след това Комисията представя доклад относно прегледа на напредъка в разработването на стандартизационни документи за ефективното от енергийна гледна точка разработване на модели на ИИ с общо предназначение и оценява необходимостта от допълнителни мерки или действия, включително задължителни мерки или действия. Докладът се предава на Европейския парламент и на Съвета и се оповестява публично.
7. До 2 август 2028 г. и на всеки три години след това Комисията оценява въздействието и ефективността на незадължителните кодекси за поведение с цел насърчаване на прилагането на изискванията, установени в глава III, раздел 2, за системи с ИИ, различни от високорисковите системи с ИИ, и евентуално на други допълнителни изисквания за системите с ИИ, различни от високорисковите системи с ИИ, включително по отношение на екологичната устойчивост.
8. Съветът по ИИ, държавите членки и националните компетентни органи предоставят на Комисията информация за целите на параграфи 1 – 7, по нейно искане и без ненужно забавяне.
9. При извършването на оценките и прегледите по параграфи 1—7 Комисията взема предвид позициите и констатациите на Съвета по ИИ, Европейския парламент, Съвета и на други компетентни органи или източници.

10. Когато е необходимо, Комисията представя подходящи предложения за изменение на настоящия регламент, като отчита по-специално развитието на технологиите, въздействието на системите с ИИ върху здравето, безопасността и основните права, както и напредъка в областта на информационното общество.

11. За да насочва оценките и прегледите, посочени в параграфи 1 – 7 от настоящия член, Службата по ИИ разработва обективна и приобщаваща методология за оценка на нивата на риска въз основа на критериите, посочени в съответните членове, и включването на нови системи във:

- а) списъка, съдържащ се в приложение III, включително разширяването на съществуващи функции в дадена област или добавянето на нови функции в дадена област в посоченото приложение;
- б) списъка на забранени практики, определени в член 5; и
- в) списъка на системите с ИИ, за които се изискват допълнителни мерки за прозрачност съгласно член 50.

12. Всяко изменение на настоящия регламент съгласно параграф 10 или на съответните делегирани актове или актове за изпълнение, което се отнася до секторното законодателство на Съюза за хармонизация, посочено в раздел Б от приложение I, трябва да е съобразено с регулаторните особености на всеки сектор и съществуващите механизми и органи за управление, оценяване на съответствието и контрол на прилагането.

13. До 2 август 2031 г. Комисията извършва оценка на осигуряването на спазването на настоящия регламент и я докладва на Европейския парламент, Съвета и Европейския икономически и социален комитет, като взема предвид първите пет години от прилагането на настоящия регламент. Въз основа на констатациите този доклад се придружава, когато е целесъобразно, от предложение за изменение на настоящия регламент по отношение на структурата на осигуряването на спазването и необходимостта от създаване на агенция на Съюза се цел отстраняване на установените недостатъци.

Член 113

Влизане в сила и прилагане

Настоящият регламент влиза в сила на двадесетия ден след публикуването му в *Официален вестник на Европейския съюз*.

Прилага се от 2 август 2026 г.

Независимо от това:

- а) глави I и II се прилагат, считано от 2 февруари 2025 г.;
- б) глава III, раздел 4, глави V, VII и XII и член 78 се прилагат, считано от 2 август 2025 г., с изключение на член 101;
- в) член 6, параграф 1 и съответните задължения в настоящия регламент се прилагат, считано от 2 август 2027 г.

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

Съставено в Брюксел на 13 юни 2024 година.

За Европейския парламент

Председател

R. METSOLA

За Съвета

Председател

M. MICHEL

ПРИЛОЖЕНИЕ I

Списък на законодателството на Съюза за хармонизация

Раздел А. Списък на законодателството на Съюза за хармонизация въз основа на новата законодателна рамка

1. Директива 2006/42/ЕО на Европейския парламент и на Съвета от 17 май 2006 г. относно машините и за изменение на Директива 95/16/ЕО (ОВ L 157, 9.6.2006 г., стр. 24) [отменена с Регламента за машините];
2. Директива 2009/48/ЕО на Европейския парламент и на Съвета от 18 юни 2009 г. относно безопасността на детските играчки (ОВ L 170, 30.6.2009 г., стр. 1);
3. Директива 2013/53/ЕС на Европейския парламент и на Съвета от 20 ноември 2013 г. относно плавателните съдове за отдых и плавателните съдове за лично ползване и за отмяна на Директива 94/25/ЕО (ОВ L 354, 28.12.2013 г., стр. 90);
4. Директива 2014/33/ЕС на Европейския парламент и на Съвета от 26 февруари 2014 г. за хармонизиране на законодателствата на държавите членки по отношение на асансьори и предпазни устройства за асансьори (ОВ L 96, 29.3.2014 г., стр. 251);
5. Директива 2014/34/ЕС на Европейския парламент и на Съвета от 26 февруари 2014 г. за хармонизиране на законодателствата на държавите членки относно съоръженията и системите за защита, предназначени за използване в потенциално експлозивна атмосфера (ОВ L 96, 29.3.2014 г., стр. 309);
6. Директива 2014/53/ЕС на Европейския парламент и на Съвета от 16 април 2014 г. за хармонизирането на законодателствата на държавите членки във връзка с предоставянето на пазара на радиосъоръжения и за отмяна на Директива 1999/5/ЕО (ОВ L 153, 22.5.2014 г., стр. 62);
7. Директива 2014/68/ЕС на Европейския парламент и на Съвета от 15 май 2014 г. за хармонизиране на законодателствата на държавите членки за предоставяне на пазара на съоръжения под налягане (ОВ L 189, 27.6.2014 г., стр. 164);
8. Регламент (ЕС) 2016/424 на Европейския парламент и на Съвета от 9 март 2016 г. относно въжените линии и за отмяна на Директива 2000/9/ЕО (ОВ L 81, 31.3.2016 г., стр. 1);
9. Регламент (ЕС) 2016/425 на Европейския парламент и на Съвета от 9 март 2016 г. относно личните предпазни средства и за отмяна на Директива 89/686/ЕО на Съвета (ОВ L 81, 31.3.2016 г., стр. 51);
10. Регламент (ЕС) 2016/426 на Европейския парламент и на Съвета от 9 март 2016 г. относно уредите, захранвани с газово гориво, и за отмяна на Директива 2009/142/ЕО (ОВ L 81, 31.3.2016 г., стр. 99);
11. 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/ЕО и 93/42/ЕО на Съвета (ОВ L 117, 5.5.2017 г., стр. 1);
12. 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).

Раздел Б. Списък на друго законодателство на Съюза за хармонизация

13. 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);
14. Регламент (ЕС) № 168/2013 на Европейския парламент и на Съвета от 15 януари 2013 г. относно одобряването и надзора на пазара на дву-, три- и четириколесни превозни средства (ОВ L 60, 2.3.2013 г., стр. 52);
15. 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);

16. 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);
17. 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);
18. 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).
19. Регламент (ЕС) 2019/2144 на Европейския парламент и на Съвета от 27 ноември 2019 г. относно изискванията за одобряване на типа на моторни превозни средства и техните ремаркета, както и на системи, компоненти и отделни технически възли, предназначени за такива превозни средства, по отношение на общата безопасност на моторните превозни средства 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 на 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) № 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);
20. 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), що се отнася до проектирането, производството и пускането на пазара на въздухоплавателните средства, посочени в член 2, параграф 1, букви а) и б) от него, когато това засяга безпилотни въздухоплавателни средства, техните двигатели, витла, части и оборудване за управлението им от разстояние.

ПРИЛОЖЕНИЕ II

Списък на престъпленията, посочени в член 5, параграф 1, първа алинея, буква з), точка iii)

Престъпления, посочени в член 5, параграф 1, първа алинея, буква з), точка iii):

- тероризъм,
- трафик на хора,
- сексуална експлоатация на деца и детска порнография,
- незаконен трафик на наркотици или психотропни вещества,
- незаконен трафик на оръжия, боеприпаси и взривни вещества,
- убийство, тежка телесна повреда,
- незаконна търговия с човешки органи или тъкани,
- незаконен трафик на ядрени или радиоактивни материали,
- отвлечане, противозаконно лишаване от свобода или задържане на заложници,
- престъпления от компетентността на Международния наказателен съд,
- незаконно отвлечане на летателни средства или кораби,
- изнасилване,
- престъпления против околната среда,
- организиран или въоръжен грабеж,
- саботаж,
- участие в престъпна организация, замесена в едно или повече от престъпленията, изброени по-горе.

ПРИЛОЖЕНИЕ III

Високорискови системи с ИИ по член 6, параграф 2

Високорискови системи с ИИ съгласно член 6, параграф 2 са системите с ИИ в някоя от следните области:

1. Биометрични данни, доколкото използването им е разрешено съгласно съответното право на Съюза или национално право:
 - а) системи за дистанционна биометрична идентификация.

Това не включва системите с ИИ, предназначени да се използват за биометрична проверка, чиято единствена цел е да потвърдят, че определено физическо лице е лицето, за което се представя;
 - б) системи с ИИ, предназначени да се използват за биометрично категоризиране въз основа на чувствителни или защитени признаци или характеристики въз основа на изводи за тези признаци или характеристики;
 - в) системи с ИИ, предназначени да се използват за разпознаване на емоции.
2. Критична инфраструктура: системи с ИИ, предназначени да се използват като защитни елементи при управлението и експлоатацията на критичната цифрова инфраструктура, движението по пътищата или водоснабдяването, газоснабдяването, отоплението или електроснабдяването.
3. Образование и професионално обучение:
 - а) системи с ИИ, предназначени да бъдат използвани за определяне на достъпа до, приема във или насочването на физически лица към институции на всички нива на образованието и професионалното обучение;
 - б) системи с ИИ, предназначени да бъдат използвани за оценяване на учебните резултати, включително когато тези резултати се използват за направляване на учебния процес на физически лица в рамките на институции на всички нива на образованието и професионалното обучение;
 - в) системи с ИИ, предназначени да се използват за оценка на подходящото ниво на образование, което дадено лице ще получи или до което ще има достъп, в контекста на или в рамките на институции на всички нива на образованието и професионалното обучение;
 - г) системи с ИИ, предназначени да се използват за наблюдение и откриване на забранено поведение на учащите по време на изпити в контекста на или в рамките на институции на всички нива на образованието и професионалното обучение.
4. Заетост, управление на работниците и достъп до самостоятелна заетост:
 - а) системи с ИИ, предназначени да бъдат използвани за набиране или подбор на физически лица, по-специално за поместване на конкретно насочени обяви за работа, за анализиране или отсяване на молби за работа и за оценяване на кандидатите;
 - б) системи с ИИ, предназначени да бъдат използвани за вземане на решения, засягащи условията на отношения във връзка с полагане на труд, повишението или прекратяването на договорни отношения във връзка с полагане на труд, за разпределяне на задачите въз основа на индивидуално поведение или личностни черти или характеристики или за наблюдение и оценяване на работата и поведението на лицата при такива правоотношения.
5. Достъп до и използване на основни частни услуги и основни публични услуги и подпомагане:
 - а) системи с ИИ, предназначени да бъдат използвани от публични органи или от името на публични органи за оценка на допустимостта на физически лица за получаване на основно обществено подпомагане и услуги, включително услуги в областта на здравеопазването, както и за отпускане, намаляване, прекратяване или възстановяване на такова подпомагане и услуги;
 - б) системи с ИИ, предназначени да се използват за оценка на кредитоспособността на физически лица или за определяне на техния кредитен рейтинг, с изключение на системите с ИИ, използвани за целите на откриване на финансови измами;
 - в) системи с ИИ, предназначени да се използват за оценка на риска и ценообразуване по отношение на физически лица в случай на животозастраховане и здравно застраховане;

- г) системи с ИИ, предназначени за оценка и класифициране на спешни повиквания от физически лица или за изпращане, или за определяне на приоритет при изпращането на службите за спешно реагиране, включително полицията, пожарната и медицинската помощ, както и на системите за разпределяне на пациенти за спешна здравна помощ;
6. Правоохранителна дейност, доколкото тяхното използване е разрешено съгласно съответното право на Съюза или национално право:
- а) системи с ИИ, предназначени да бъдат използвани от правоохранителните органи или от тяхно име, или от институции, органи, служби и агенции на Съюза в подкрепа на правоохранителните органи или от тяхно име с цел оценка на риска физическо лице да стане жертва на престъпления;
- б) системи с ИИ, предназначени да бъдат използвани от правоохранителните органи или от тяхно име, или от институции, органи, служби и агенции на Съюза в подкрепа на правоохранителните органи като полиграфи или подобни инструменти;
- в) системи с ИИ, предназначени да бъдат използвани от правоохранителните органи или от тяхно име, или от институции, органи, служби и агенции на Съюза в подкрепа на правоохранителните органи за оценка на надеждността на доказателствата в хода на разследването или наказателното преследване на престъпления;
- г) системи с ИИ, предназначени да бъдат използвани от правоохранителните органи или от тяхно име, или от институции, органи, служби и агенции на Съюза в подкрепа на правоохранителните органи за оценка на риска дадено физическо лице да извърши нарушение или повторно нарушение не само въз основа на профилиране на физически лица, както е посочено в член 3, параграф 4 от Директива (ЕС) 2016/680, или за оценка на личностните черти и характеристики или на минало престъпно поведение на физически лица или групи;
- д) системи с ИИ, предназначени да бъдат използвани от правоохранителните органи или от тяхно име, или от институции, органи, служби и агенции на Съюза в подкрепа на правоохранителните органи за профилиране на физически лица, както е посочено в член 3, параграф 4 от Директива (ЕС) 2016/680, в хода на разкриването, разследването или наказателното преследване на престъпления.
7. Управление на миграцията, убежището и граничния контрол, доколкото тяхното използване е разрешено съгласно съответното право на Съюза или национално право:
- а) системи с ИИ, предназначени да бъдат използвани от компетентните публични органи или от тяхно име, или от институции, органи, служби или агенции на Съюза като полиграфи или подобни инструменти;
- б) системи с ИИ, предназначени да бъдат използвани от компетентните публични органи или от тяхно име, или от институции, органи, служби или агенции на Съюза за оценка на риск, включително риск за сигурността, риск от незаконна миграция или риск за здравето, породен от физическо лице, което възнамерява да влезе или е влязло на територията на държава членка;
- в) системи с ИИ, предназначени да бъдат използвани от компетентните публични органи или от тяхно име, или от институции, органи, служби или агенции на Съюза 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 допустимостта на физическите лица, кандидатстващи за статут, включително свързани оценки на надеждността на доказателствата;
- г) системи с ИИ, предназначени да се използват от компетентните публични органи или от тяхно име, или от институции, органи, служби или агенции на Съюза, в контекста на управлението на миграцията, убежището или граничния контрол, с цел откриване, разпознаване или установяване на самоличността на физически лица, с изключение на проверката на документи за пътуване.
8. Правораздаване и демократични процеси:
- а) системи с ИИ, предназначени да бъдат използвани от орган на съдебната власт или от негово име за подпомагане на орган на съдебната власт при проучване и тълкуване на фактите и правото и при прилагане на закона към конкретен набор от факти, или за използване по подобен начин при алтернативно решаване на спорове;

- б) системи с ИИ, предназначени да бъдат използвани за оказване на влияние върху резултата от избори или референдум или върху поведението на физическите лица при упражняване на правото им на глас в избори или референдум. Това не включва системи с ИИ, на чиито резултати физическите лица не са пряко изложени, като инструменти, използвани за организиране, оптимизиране и структуриране на политически кампании от административна или логистична гледна точка.
-

ПРИЛОЖЕНИЕ IV

Техническа документация по член 11, параграф 1

Техническата документация по член 11, параграф 1 съдържа най-малко следната информация, както е приложимо за съответната система с ИИ:

1. Общо описание на системата с ИИ, включително:
 - а) предназначението ѝ, името на доставчика и версията на системата, отразяваща връзката ѝ с предишни версии;
 - б) как системата с ИИ взаимодейства или може да се използва за взаимодействие с хардуер или софтуер, включително с други системи с ИИ, които не са част от самата система с ИИ, когато е приложимо;
 - в) версиите на съответния софтуер или фърмуер и всички изисквания, свързани с актуализирането на версиите;
 - г) описание на всички форми, под които системата с ИИ се пуска на пазара или се пуска в действие, например софтуерни пакети, вградени в хардуер, продукти, които могат да бъдат изтеглени, или API;
 - д) описание на хардуера, на който се предвижда да работи системата с ИИ;
 - е) когато системата с ИИ е компонент от продукти — снимки или илюстрации, показващи външни характеристики, маркировка и вътрешно оформление на тези продукти;
 - ж) основно описание на потребителския интерфейс, предоставен на внедрителя;
 - з) инструкциите за употреба за внедрителя, и основно описание на потребителския интерфейс, предоставен на внедрителя, когато е приложимо;
2. Подробно описание на елементите на системата с ИИ и на процеса за нейното разработване, включително:
 - а) методите и стъпките за разработването на системата с ИИ, включително, когато е приложимо, използването на предварително обучени системи или инструменти, предоставени от трети лица, и как те са били използвани, интегрирани или променени от доставчика;
 - б) проектните спецификации на системата и по-специално общата логика на системата с ИИ и на алгоритмите; ключовите проектантски решения, включително обосновката и направените допускания, включително по отношение на лицата или групите лица, по отношение на които се планира да се използва системата; основните варианти за класификация; какво е проектирана да оптимизира системата и адекватността на различните параметри; описанието на очакваните резултати и качеството на резултатите на системата; решенията за евентуални компромиси по отношение на техническите решения, приети с цел спазване на изискванията, установени в глава III, раздел 2;
 - в) описание на архитектурата на системата, в което се обяснява как софтуерните компоненти се надграждат или допълват взаимно и как се интегрират в цялостната обработка; изчислителните ресурси, използвани за разработване, обучение, изпитване и валидиране на системата с ИИ;
 - г) когато е приложимо, изискванията за данните под формата на информационни фишове, описващи използваните методики и техники на обучение и набори от обучителни данни, включително общо описание на тези набори от данни, информация за произхода им, техния обхват и основни характеристики; как са получени и подбрани данните; процедури за обозначаване (например за обучение с надзор), техники за изчистване на данни (например откриване на отдалечаващи се стойности);
 - д) оценка на мерките за упражняване на човешки контрол, необходими в съответствие с член 14, включително оценка на техническите мерки, необходими за улесняване на тълкуването на резултатите от системите с ИИ от внедрителите, в съответствие с член 13, параграф 3, буква г);
 - е) когато е приложимо, подробно описание на предварително заложените промени в системата с ИИ и нейните показатели, заедно с цялата съответна информация, свързана с техническите решения, приети за осигуряване на непрекъснато съответствие на системата с ИИ с приложимите изисквания, установени в глава III, раздел 2;
 - ж) използваните процедури за валидиране и изпитване, включително информация за използваните валидационни и изпитвателни данни и техните основни характеристики; показатели, използвани за измерване на точността, стабилността и спазването на други приложими изисквания, определени в глава III, раздел 2, както и потенциално дискриминационното въздействие; записите и всички протоколи от изпитвания с дата и подпис на отговорните лица, включително по отношение на предварително заложените промени, посочени в буква е);

- з) въведените мерки за киберсигурност;
3. Подробна информация относно мониторинга, функционирането и контрола на системата с ИИ, по-специално по отношение на: нейните способности и ограничения на работа, включително степените на точност за конкретни лица или групи лица, за които се предвижда да се използва системата, и общото очаквано ниво на точност по отношение на предназначението ѝ; предвидимите нежелани резултати и източници на рискове за здравето и безопасността, основните права и дискриминацията с оглед на предназначението на системата с ИИ; мерките за упражняване на човешки контрол, необходими в съответствие с член 14, включително техническите мерки, въведени за улесняване на тълкуването на резултатите от системите с ИИ от внедрителите; спецификации на входящите данни, в зависимост от случая;
 4. Описание на целесъобразността на показателите за ефективност за конкретната система с ИИ;
 5. Подробно описание на системата за управление на риска в съответствие с член 9;
 6. Описание на съответните изменения в системата, извършени от доставчика през жизнения ѝ цикъл;
 7. Списък на хармонизираните стандарти, приложени изцяло или частично, за които е публикувана справочна информация в *Официален вестник на Европейския съюз*; когато не са приложени такива хармонизирани стандарти — подробно описание на решенията, приети за изпълнение на изискванията, установени в глава III, раздел 2, включително списък на приложените други съответни стандарти и технически спецификации;
 8. Копие на ЕС декларацията за съответствие, посочена в член 47;
 9. Подробно описание на въведената система за оценка на функционирането на системата с ИИ на етапа след пускането на пазара в съответствие с член 72, включително плана за мониторинг след пускането на пазара по член 72, параграф 3.
-

ПРИЛОЖЕНИЕ V

ЕС декларация за съответствие

ЕС декларацията за съответствие по член 47 съдържа цялата посочена по-долу информация:

1. Наименование и вид на системата с ИИ и всяка допълнителна недвусмислена справочна информация, позволяваща идентифициране и проследимост на системата с ИИ;
2. Име и адрес на доставчика или, когато е приложимо, на неговия упълномощен представител;
3. Заявление, че ЕС декларацията за съответствие, посочена в член 47, е изготвена единствено на отговорността на доставчика;
4. Заявление, че системата с ИИ е в съответствие с настоящия регламент и ако е приложимо, с всяко друго съответно право на Съюза, което предвижда изготвянето на ЕС декларацията за съответствие, посочена в член 47;
5. Когато дадена система с ИИ включва обработване на лични данни — декларация, че тази система с ИИ е в съответствие с регламенти (ЕС) 2016/679 и (ЕС) 2018/1725 и Директива (ЕС) 2016/680;
6. Позовавания на всички използвани съответни хармонизирани стандарти или на всяка друга обща спецификация, по отношение на която се декларира съответствие;
7. Когато е приложимо, наименование и идентификационен номер на нотифицирания орган, описание на извършената процедура за оценяване на съответствието и идентификация на издадения сертификат;
8. Място и дата на издаване на декларацията, име и длъжност на лицето, което я е подписало, както и указание за кого или от чие име е подписало това лице, и подпис.

ПРИЛОЖЕНИЕ VI

Процедура за оценяване на съответствието въз основа на вътрешен контрол

1. Процедурата за оценяване на съответствието въз основа на вътрешен контрол е процедурата за оценяване на съответствието въз основа на точки 2, 3 и 4.
 2. Доставчикът проверява дали установената система за управление на качеството е в съответствие с изискванията по член 17.
 3. Доставчикът проверява информацията, съдържаща се в техническата документация, за да оцени съответствието на системата с ИИ с приложимите съществени изисквания, установени в глава III, раздел 2.
 4. Доставчикът също така проверява дали процесът на проектиране и разработване на системата с ИИ и нейният мониторинг след пускането на пазара по член 72 са в съответствие с техническата документация.
-

ПРИЛОЖЕНИЕ VII

Съответствие въз основа на оценка на системата за управление на качеството и оценка на техническата документация

1. Въведение

Съответствие въз основа на оценка на системата за управление на качеството и оценка на техническата документация е процедурата за оценяване на съответствието въз основа на точки 2—5.

2. Преглед

Одобрената система за управление на качеството за проектирането, разработването и изпитването на системи с ИИ съгласно член 17 се разглежда в съответствие с точка 3 и подлежи на надзор съгласно точка 5. Техническата документация на системата с ИИ се проверява в съответствие с точка 4.

3. Система за управление на качеството

3.1. Заявлението на доставчика включва:

- а) името и адреса на доставчика, а в случаите, когато заявлението е подадено от упълномощен представител — и неговото име и адрес;
- б) списъка на системите с ИИ, обхванати от една и съща система за управление на качеството;
- в) техническата документация за всяка система с ИИ, обхваната от една и съща система за управление на качеството;
- г) документацията относно системата за управление на качеството, която обхваща всички аспекти, изброени в член 17;
- д) описание на въведените процедури, за да се гарантира, че системата за управление на качеството продължава да бъде адекватна и ефективна;
- е) писмена декларация, че същото заявление не е било подавано до друг нотифициран орган.

3.2. Системата за управление на качеството се оценява от нотифицирания орган, който определя дали тя отговаря на изискванията по член 17.

Решението се съобщава на доставчика или на неговия упълномощен представител.

Уведомлението съдържа заключенията от оценката на системата за управление на качеството и мотивираното решение от оценката.

3.3. Одобрената система за управление на качеството продължава да се прилага и поддържа от доставчика така, че да продължи да бъде адекватна и ефикасна.

3.4. Доставчикът уведомява нотифицирания орган за всяка планирана промяна в одобрената система за управление на качеството или в списъка на системите с ИИ, обхванати от нея.

Предложените промени се разглеждат от нотифицирания орган, който решава дали променената система за управление на качеството продължава да отговаря на изискванията по точка 3.2, или се налага ново оценяване.

Нотифицираният орган съобщава решението си на доставчика. Уведомлението съдържа заключенията от разглеждането на промените и мотивираното решение от оценката.

4. Контрол на техническата документация.

4.1. В допълнение към заявлението по точка 3 доставчикът подава заявление до нотифициран орган по негов избор за оценка на техническата документация, свързана със системата с ИИ, която доставчикът възнамерява да пусне на пазара или да пусне в действие и която е обхваната от системата за управление на качеството по точка 3.

4.2. Заявлението включва:

- а) името и адреса на доставчика;
- б) писмена декларация, че същото заявление не е било подавано до друг нотифициран орган;
- в) техническата документация по приложение IV.

- 4.3. Техническата документация се разглежда от нотифицирания орган. Когато е приложимо и в рамките на необходимото за изпълнение на задачите му, нотифицираният орган получава пълен достъп до наборите от използвани обучителни, валидационни и изпитвателни данни, включително, когато е целесъобразно и при наличие на гаранции за сигурността, чрез API или други подходящи технически средства и инструменти, позволяващи дистанционен достъп.
- 4.4. При разглеждането на техническата документация нотифицираният орган може да изиска доставчикът да предостави допълнителни доказателства или да извърши допълнителни изпитвания, за да даде възможност за правилно оценяване на съответствието на системата с ИИ с изискванията, установени в глава III, раздел 2. Когато нотифицираният орган не е удовлетворен от изпитванията, проведени от доставчика, самият той провежда директно подходящи изпитвания, доколкото е целесъобразно.
- 4.5. Когато е необходимо за оценяване на съответствието на високорисковата система с ИИ с изискванията, установени в глава III, раздел 2, след като всички други разумни начини за проверка на съответствието са били изчерпани или са се оказали недостатъчни, и при обосновано искане, на нотифицирания орган се предоставя и достъп до учебните и обучените модели на системата с ИИ, включително съответните параметри на модела. По отношение на този достъп се прилага съществуващото право на Съюза относно закрилата на интелектуалната собственост и търговските тайни.
- 4.6. Решението на нотифицирания орган се съобщава на доставчика или на неговия упълномощен представител. Уведомлението съдържа заключенията от оценката на техническата документация и мотивираното решение от оценката.

Когато системата с ИИ е в съответствие с изискванията, установени в глава III, раздел 2, нотифицираният орган издава сертификат на Съюза за оценяване на техническата документация. В сертификата се указват името и адресът на доставчика, заключенията от разглеждането, условията (ако има такива) за неговата валидност и необходимите данни за идентифициране на системата с ИИ.

Сертификатът и приложенията към него съдържат цялата необходима информация, за да може да се оцени съответствието на системата с ИИ и да се даде възможност за контрол на системата с ИИ по време на използването ѝ, когато е приложимо.

Когато системата с ИИ не съответства на изискванията, установени в глава III, раздел 2, нотифицираният орган отказва да издаде сертификат на Съюза за оценяване на техническата документация и информира заявителя за това, като подробно описва причините за отказа си.

Когато системата с ИИ не отговаря на изискването, свързано с данните, използвани за нейното обучение, е необходимо повторно обучение на системата с ИИ преди подаването на заявление за ново оценяване на съответствието. В този случай мотивираното решение от оценката, с което нотифицираният орган отказва да издаде сертификат на Съюза за оценяване на техническата документация, съдържа конкретни съображения относно качествените данни, използвани за обучение на системата с ИИ, по-специално относно причините за несъответствието.

- 4.7. Всяка промяна в системата с ИИ, която би могла да засегне съответствието на системата с ИИ с изискванията или предназначението ѝ, се оценява от нотифицирания орган, който е издал сертификата на Съюза за оценяване на техническата документация. Доставчикът информира този нотифициран орган за намерението си да въведе някоя от горепосочените промени или ако узнае по друг начин за настъпването на такива промени. Нотифицираният орган оценява планираните промени и решава дали те изискват ново оценяване на съответствието в съответствие с член 43, параграф 4, или въпросът може да бъде решен чрез допълнение към сертификата на Съюза за оценяване на техническата документация. В последния случай нотифицираният орган оценява промените, уведомява доставчика за своето решение и ако промените са одобрени, издава на доставчика допълнение към сертификата на Съюза за оценяване на техническата документация.
5. Надзор на одобрената система за управление на качеството.
- 5.1. Целта на надзора, осъществяван от нотифицирания орган по точка 3, е да се гарантира, че доставчикът спазва надлежно реда и условията на одобрената система за управление на качеството.
- 5.2. За целите на оценяването доставчикът разрешава на нотифицирания орган достъп до помещенията, в които се извършват проектирането, разработването и изпитването на системите с ИИ. Освен това доставчикът споделя с нотифицирания орган цялата необходима информация.
- 5.3. Нотифицираният орган периодично извършва одити, за да се увери, че доставчикът поддържа и прилага системата за управление на качеството, и предоставя на доставчика доклад от одита. В контекста на тези одити нотифицираният орган може да извършва допълнителни изпитвания на системите с ИИ, за които е издаден сертификат на Съюза за оценяване на техническата документация.

ПРИЛОЖЕНИЕ VIII

Информация, която се подава при регистрацията на високорискови системи с ИИ в съответствие с член 49

Раздел А — Информация, която се подава от доставчиците на високорискови системи с ИИ в съответствие с член 49, параграф 1

По отношение на високорисковите системи с ИИ, които се регистрират в съответствие с член 49, параграф 1, се предоставя и впоследствие се поддържа актуална следната информация:

1. Име, адрес и данни за контакт на доставчика;
2. Когато предоставянето на информация се извършва от друго лице от името на доставчика — име, адрес и данни за контакт на това лице;
3. Име, адрес и данни за контакт на упълномощения представител, когато е приложимо;
4. Търговско наименование на системата с ИИ и всяка допълнителна недвусмислена справочна информация, позволяваща идентифициране и проследяване на системата с ИИ;
5. Описание на предназначението на системата с ИИ и на компонентите и функциите, поддържани чрез тази система с ИИ;
6. Основно и кратко описание на информацията, използвана от системата (данни, входящи данни), и нейната работна логика;
7. Статус на системата с ИИ (на пазара или в действие; вече не се пуска на пазара/не е в действие, иззета);
8. Вид, номер и дата на изтичане на валидността на сертификата, издаден от нотифицирания орган, и наименование или идентификационен номер на този нотифициран орган, когато е приложимо;
9. Сканирано копие на сертификата по точка 8, когато е приложимо;
10. Държавите членки, в които системата с ИИ е била пусната на пазара, пусната в действие или предоставена в Съюза;
11. Копие на ЕС декларацията за съответствие по член 47;
12. Електронни инструкции за употреба; тази информация не се предоставя за високорискови системи с ИИ в правоохранителната област или в областите на управлението на миграцията, убежището и граничния контрол, посочени в приложение III, точки 1, 6 и 7.
13. Уеб адрес (URL) за допълнителна информация (незадължително).

Раздел Б — Информация, която се подава от доставчиците на високорискови системи с ИИ в съответствие с член 49, параграф 2

По отношение на системите с ИИ, които се регистрират в съответствие с член 49, параграф 2, се предоставя и впоследствие се поддържа актуална следната информация:

1. Име, адрес и данни за контакт на доставчика;
2. Когато предоставянето на информация се извършва от друго лице от името на доставчика — име, адрес и данни за контакт на това лице;
3. Име, адрес и данни за контакт на упълномощения представител, когато е приложимо;
4. Търговско наименование на системата с ИИ и всяка допълнителна недвусмислена справочна информация, позволяваща идентифициране и проследимост на системата с ИИ;
5. Описание на предназначението на системата с ИИ;
6. Условието или условията съгласно член 6, параграф 3, въз основа на които се счита, че системата с ИИ не е високорискова;
7. Кратко обобщение на основанията, въз основа на които системата с ИИ не се счита за високорискова при прилагането на процедурата по член 6, параграф 3;
8. Статус на системата с ИИ (на пазара или в действие; вече не се пуска на пазара/не е в действие, иззета);
9. Държави членки, в които системата с ИИ е била пусната на пазара, пусната в действие или предоставена в Съюза.

Раздел В — Информация, която се подава от внедрителите на високорискови системи с ИИ в съответствие с член 49, параграф 3

По отношение на високорисковите системи с ИИ, които се регистрират в съответствие с член 49, се предоставя и впоследствие се поддържа актуална следната информация:

1. Име, адрес и данни за контакт на внедрителя;
 2. Име, адрес и данни за контакт на всяко лице, което подава информация от името на внедрителя;
 3. Уеб адрес (URL) на вписването на системата с ИИ в базата данни на ЕС от нейния доставчик;
 4. Обобщение на констатациите от оценката на въздействието върху основните права, извършена в съответствие с член 27;
 5. Обобщение на оценката на въздействието върху защитата на данните, извършена в съответствие с член 35 от Регламент (ЕС) 2016/679 или член 27 от Директива (ЕС) 2016/680, както е посочено в член 26, параграф 8 от настоящия регламент, когато е приложимо.
-

ПРИЛОЖЕНИЕ IX

Информация, която се подава при регистрацията на високорисковите системи с ИИ, изброени в приложение III, във връзка с изпитване в реални условия в съответствие с член 60

Във връзка с изпитването в реални условия, което се регистрира в съответствие с член 60, се предоставя и впоследствие се актуализира следната информация:

1. Уникален единен идентификационен номер в рамките на Съюза на изпитването в реални условия;
 2. Име и данни за контакт на доставчика или потенциалния доставчик и на внедрителите, участващи в изпитването в реални условия;
 3. Кратко описание на системата с ИИ, нейното предназначение и друга информация, необходима за идентифицирането на системата;
 4. Обобщение на основните характеристики на плана за изпитване в реални условия;
 5. Информация за спирането или прекратяването на изпитването в реални условия.
-

ПРИЛОЖЕНИЕ X

Законодателни актове на Съюза относно широкомащабни информационни системи в пространството на свобода, сигурност и правосъдие

1. Шенгенска информационна система

- а) Регламент (ЕС) 2018/1860 на Европейския парламент и на Съвета от 28 ноември 2018 г. за използването на Шенгенската информационна система за целите на връщането на незаконно пребиваващи граждани на трети държави (ОБ L 312, 7.12.2018 г., стр. 1),
- б) Регламент (ЕС) 2018/1861 на Европейския парламент и на Съвета от 28 ноември 2018 г. за създаването, функционирането и използването на Шенгенската информационна система (ШИС) в областта на граничните проверки, за изменение на Конвенцията за прилагане на Споразумението от Шенген и за изменение и отмяна на Регламент (ЕО) № 1987/2006 (ОБ L 312, 7.12.2018 г., стр. 14),
- в) Регламент (ЕС) 2018/1862 на Европейския парламент и на Съвета от 28 ноември 2018 г. за създаването, функционирането и използването на Шенгенската информационна система (ШИС) в областта на полицейското сътрудничество и съдебното сътрудничество по наказателноправни въпроси, за изменение и отмяна на Решение 2007/533/ПВР на Съвета и за отмяна на Регламент (ЕО) № 1986/2006 на Европейския парламент и на Съвета и Решение 2010/261/ЕС на Комисията (ОБ L 312, 7.12.2018 г., стр. 56).

2. Визова информационна система

- а) Регламент (ЕС) 2021/1133 на Европейския парламент и на Съвета от 7 юли 2021 г. за изменение на регламенти (ЕС) № 603/2013, (ЕС) 2016/794, (ЕС) 2018/1862, (ЕС) 2019/816 и (ЕС) 2019/818 по отношение на установяването на условията за достъп до други информационни системи на ЕС за целите на Визовата информационна система (ОБ L 248, 13.7.2021 г., стр. 1),
- б) Регламент (ЕС) 2021/1134 на Европейския парламент и на Съвета от 7 юли 2021 г. за изменение на регламенти (ЕО) № 767/2008, (ЕО) № 810/2009, (ЕС) 2016/399, (ЕС) 2017/2226, (ЕС) 2018/1240, (ЕС) 2018/1860, (ЕС) 2018/1861, (ЕС) 2019/817 и (ЕС) 2019/1896 на Европейския парламент и на Съвета и за отмяна на решения 2004/512/ЕО и 2008/633/ПВР на Съвета за целите на реформирането на Визовата информационна система (ОБ L 248, 13.7.2021 г., стр. 11).

3. Евродак

Регламент (ЕС) 2024/1358 на Европейския парламент и на Съвета от 14 май 2024 г. за създаване на системата Евродак за сравняване на биометрични данни с цел ефективно прилагане на регламенти (ЕС) 2024/1315 и (ЕС) 2024/1350 на Европейския парламент и на Съвета и на Директива 2001/55/ЕО на Съвета и установяване на самоличността на незаконно пребиваващи граждани на трета държава и лица без гражданство и относно искания за сравняване с данните в Евродак, отправени от правоприлагащите органи на държавите членки и Европол за целите на правоприлагането, за изменение на регламенти (ЕС) 2018/1240 и (ЕС) 2019/818 на Европейския парламент и на Съвета и за отмяна на Регламент (ЕС) № 603/2013 на Европейския парламент и на Съвета (ОБ L, 2024/1358, 22.5.2024 г., ELI: <https://eur-lex.europa.eu/eli/reg/2024/1358/oj>).

4. Система за влизане/излизане

Регламент (ЕС) 2017/2226 на Европейския парламент и на Съвета от 30 ноември 2017 г. за създаване на Система за влизане/излизане (СВИ) с цел регистриране на данните относно влизането и излизането и данните относно отказа за влизане на граждани на трети страни, преминаващи външните граници на държавите членки, за определяне на условията за достъп до СВИ за целите на правоприлагането и за изменение на Конвенцията за прилагане на Шенгенското споразумение и регламенти (ЕО) № 767/2008 и (ЕС) № 1077/2011 (ОБ L 327, 9.12.2017 г., стр. 20).

5. Система на ЕС за информация за пътуванията и разрешаването им

- а) Регламент (ЕС) 2018/1240 на Европейския парламент и на Съвета от 12 септември 2018 г. за създаване на Европейска система за информация за пътуванията и разрешаването им (ETIAS) и за изменение на регламенти (ЕС) № 1077/2011, (ЕС) № 515/2014, (ЕС) 2016/399, (ЕС) 2016/1624 и (ЕС) 2017/2226 (ОБ L 236, 19.9.2018 г., стр. 1),
- б) Регламент (ЕС) 2018/1241 на Европейския парламент и на Съвета от 12 септември 2018 г. за изменение на Регламент (ЕС) 2016/794 за целите на създаването на Европейска система за информация за пътуванията и разрешаването им (ETIAS) (ОБ L 236, 19.9.2018 г., стр. 72).

6. Европейска информационна система за съдимост за граждани на трети държави и лица без гражданство
Регламент (ЕС) 2019/816 на Европейския парламент и Съвета от 17 април 2019 г. за създаване на централизирана система за установяване на държавите членки, разполагащи с информация за присъди срещу граждани на трети държави и лица без гражданство (ECRIS-TCN), с цел допълване на Европейската информационна система за съдимост и за изменение на Регламент (ЕС) 2018/1726 (ОВ L 135, 22.5.2019 г., стр. 1).
 7. Оперативна съвместимост
 - а) Регламент (ЕС) 2019/817 на Европейския парламент и на Съвета от 20 май 2019 г. за създаване на рамка за оперативна съвместимост между информационните системи на ЕС в областта на границите и визите и за изменение на регламенти (ЕО) № 767/2008, (ЕС) 2016/399, (ЕС) 2017/2226, (ЕС) 2018/1240, (ЕС) 2018/1726 и (ЕС) 2018/1861 на Европейския парламент и на Съвета и на решения 2004/512/ЕО и 2008/633/ПВР на Съвета (ОВ L 135, 22.5.2019 г., стр. 27),
 - б) Регламент (ЕС) 2019/818 на Европейския парламент и на Съвета от 20 май 2019 г. за създаване на рамка за оперативна съвместимост между информационните системи на ЕС в областта на полицейското и съдебното сътрудничество, убежището и миграцията и за изменение на регламенти (ЕС) 2018/1726, (ЕС) 2018/1862 и (ЕС) 2019/816 (ОВ L 135, 22.5.2019 г., стр. 85).
-

ПРИЛОЖЕНИЕ XI

Техническа документация по член 53, параграф 1, буква а) — техническа документация за доставчиците на модели на ИИ с общо предназначение

Раздел 1

Информация, която се предоставя от всички доставчици на модели на ИИ с общо предназначение

Техническата документация по член 53, параграф 1, буква а) съдържа най-малко следната информация, до степента, в която е целесъобразно предвид размера и рисковия профил на модела:

1. Общо описание на модела на ИИ с общо предназначение, включително:
 - а) задачите, които моделът е предназначен да изпълнява, и вида и естеството на системите с ИИ, в които той може да бъде интегриран;
 - б) приложимите политики за приемливо използване;
 - в) датата на пускане и методите на разпространение;
 - г) архитектурата и броя на параметрите;
 - д) вида (например текст, изображение) и формата на входящите и изходящите данни;
 - е) лицензът.
2. Подробно описание на елементите на модела, посочени в точка 1, и съответната информация за процеса на разработване, включително следните елементи:
 - а) техническите средства (например инструкции за употреба, инфраструктура, инструменти), необходими за интегрирането на модела на ИИ с общо предназначение в системите с ИИ;
 - б) проектните спецификации на модела и процеса на обучение, включително методологии и техники за обучение, ключовите проектни решения, включително обосновката и направените допускания; какво е проектиран да оптимизира моделът и адекватността на различните параметри, доколкото е приложимо;
 - в) информация относно данните, използвани за обучение, изпитване и валидиране, когато е приложимо, включително вида и произхода на данните и методиките за поддържане (например почистване, филтриране и т.н.), броя на данните, техният обхват и основни характеристики; как са получени и подбрани данните, както и всички други мерки за откриване на непригодност на източниците на данни и методите за откриване на установима предубеденост, когато е приложимо;
 - г) изчислителните ресурси, използвани за обучение на модела (например брой операции с плаваща запетая), времето за обучение и други съответни подробности, свързани с обучението;
 - д) известно или прогнозно енергопотребление на модела.

По отношение на буква д), когато енергопотреблението на модела е неизвестно, енергопотреблението може да се основава на информация за използваните изчислителни ресурси.

Раздел 2

Допълнителна информация, която се предоставя от доставчиците на модели на ИИ с общо предназначение, пораждащи системен риск

1. Подробно описание на стратегиите за оценка, включително резултатите от оценката, въз основа на наличните протоколи и инструменти за публична оценка или други методологии за оценка. Стратегиите за оценка включват критерии за оценка, показатели и методология за определяне на ограниченията.
2. Когато е приложимо, подробно описание на мерките, въведени с цел провеждане на вътрешно и/или външно състезателно изпитване (например техники за проверка), адаптиране на модела, включително подравняване и фино регулиране.

3. Когато е приложимо, подробно описание на архитектурата на системата, в което се обяснява как софтуерните компоненти се надграждат или допълват взаимно и как се интегрират в цялостната обработка.
-

ПРИЛОЖЕНИЕ XII

Информация за прозрачност почлен 53, параграф 1, буква б) — техническа документация за доставчиците на модели на ИИ с общо предназначение за доставчици надолу по веригата, които интегрират модела в своята система с ИИ

Информацията по член 53, параграф 1, буква б) обхваща най-малкото следните елементи:

1. Общо описание на модела на ИИ с общо предназначение, включително:
 - а) задачите, които моделът е предназначен да изпълнява, и вида и естеството на системите с ИИ, в които може да бъде интегриран;
 - б) приложимите политики за приемливо използване;
 - в) датата на пускане и методите на разпространение;
 - г) как моделът взаимодейства или може да се използва за взаимодействие с хардуер или софтуер, който не е част от самия модел, когато е приложимо;
 - д) версиите на съответния софтуер, свързани с използването на модела на ИИ с общо предназначение, когато е приложимо;
 - е) архитектурата и броя на параметрите;
 - ж) вида (например текст, изображение) и формата на входящите и изходящите данни;
 - з) лицензът за модела.
2. Описание на елементите на модела и на процеса за неговото разработване, включително:
 - а) техническите средства (например инструкции за употреба, инфраструктура, инструменти), необходими за интегрирането на модела на ИИ с общо предназначение в системите с ИИ;
 - б) вида (например текст, изображение и т.н.) и формата на входящите и изходящите данни и техния максимален размер (например дължина на контекстуалния прозорец и др.);
 - в) информация за данните, използвани за обучение, изпитване и валидиране, когато е приложимо, включително вида и произхода на данните и методиките за поддържане.

ПРИЛОЖЕНИЕ XIII

Критерии за определянето на модели на ИИ с общо предназначение, пораждащи системен риск, посочени член 51

За да определи, че даден модел на ИИ с общо предназначение има способности или въздействие, равностойни на посочените в член 51, параграф 1, буква а), Комисията взема предвид следните критерии:

- а) броя на параметрите на модела;
- б) качеството или размера на набора от данни, например измерени чрез токени;
- в) обема на изчисленията, използвани за обучение на модела, измерен в брой операции с плаваща запетая или посочен чрез комбинация от други променливи, като например прогнозни разходи за обучение, прогнозно време, необходимо за обучението, или прогнозно енергопотребление за целите на обучението;
- г) входните и изходните параметри на модела, например текст към текст (големи езикови модели), текст към изображение, мултимодалност и прагове, съобразени с най-съвременните технически постижения, за определяне на способностите с висока степен на въздействие за всеки вид параметри, както и конкретния вид входящи и изходящи данни (например биологични секвенции);
- д) сравнителните показатели и оценките на способностите на модела, включително като се вземат предвид броят на задачите без допълнително обучение, адаптивността за изучаване на нови, различни задачи, степента му на автономност и мащабируемост, инструментите, до които той има достъп;
- е) дали оказва силно въздействие върху вътрешния пазар поради своя обхват, което се предполага, когато е бил предоставен на най-малко 10 000 регистрирани бизнес ползватели, установени в Съюза;
- ж) броя на регистрираните крайни ползватели.