Акт про штучний інтелект ЄС повний текст українською

Неофіційний переклад для читання та навігації

Онлайн: https://adopta.com.ua/eu-ai-act-uk.html

Гайд для бізнесу: https://adopta.com.ua/ai-act-ukraine.html

Оригінал EUR-Lex: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32024R1689

Згенеровано: 2026-08-15

Disclaimer: матеріал ознайомчий. Це неофіційний переклад і не замінює юридичну консультацію та офіційні тексти EUR-Lex / Офіційного вісника ЄС. Підготовлено Adopta.

Зміст

Заголовок регламенту

Преамбула

Розділ I — Загальні положення

Ст. 1 · Предмет регулювання

Ст. 2 · Сфера застосування

Ст. 3 · Визначення

Ст. 4 · Освіченість у сфері ШІ

Розділ II — Заборонені практики

Ст. 5 · Заборонені практики ШІ

Розділ III — Високоризикові системи ШІ

Ст. 6 · Правила класифікації для високоризикованих систем ШІ

Ст. 7 · Зміни до Додатку III

Ст. 8 · Відповідність вимогам

Ст. 9 · Система управління ризиками

Ст. 10 · Дані та управління даними

Ст. 11 · Технічна документація

Ст. 12 · Ведення записів

Ст. 13 · Прозорість та надання інформації суб'єктам розгортання

Ст. 14 · Людський нагляд

Ст. 15 · Точність, надійність та кібербезпека

Ст. 16 · Зобов'язання постачальників високоризикованих систем ШІ

Ст. 17 · Система управління якістю

Ст. 18 · Зберігання документації

Ст. 19 · Автоматично згенеровані журнали

Ст. 20 · Коригувальні заходи та обов'язок надання інформації

Ст. 21 · Співпраця з компетентними органами

Ст. 22 · Уповноважені представники постачальників високоризикованих систем ШІ

Ст. 23 · Зобов'язання імпортерів

Ст. 24 · Зобов'язання дистриб'юторів

Ст. 25 · Відповідальності в ланцюжку створення вартості ШІ

Ст. 26 · Зобов'язання суб'єктів розгортання високоризикованих систем ШІ

Ст. 27 · Оцінка впливу на основні права для високоризикованих систем ШІ

Ст. 28 · Повідомляючі органи

Ст. 29 · Подання заяви органом оцінки відповідності для нотифікації

Ст. 30 · Процедура нотифікації

Ст. 31 · Вимоги до нотифікованих органів

Ст. 32 · Презумпція відповідності вимогам щодо нотифікованих органів

Ст. 33 · Дочірні підприємства нотифікованих органів та субпідряд

Ст. 34 · Операційні зобов'язання нотифікованих органів

Ст. 35 · Ідентифікаційні номери та переліки нотифікованих органів

Ст. 36 · Зміни до нотифікацій

Ст. 37 · Оскарження компетентності нотифікованих органів

Ст. 38 · Координація нотифікованих органів

Ст. 39 · Органи оцінки відповідності третіх країн

Ст. 40 · Гармонізовані стандарти та результати стандартизації

Ст. 41 · Загальні специфікації

Ст. 42 · Презумпція відповідності певним вимогам

Ст. 43 · Оцінка відповідності

Ст. 44 · Сертифікати

Ст. 45 · Інформаційні зобов'язання нотифікованих органів

Ст. 46 · Відступ від процедури оцінки відповідності

Ст. 47 · Декларація відповідності ЄС

Ст. 48 · Маркування CE

Ст. 49 · Реєстрація

Розділ IV — Прозорість

Ст. 50 · Зобов'язання щодо прозорості для постачальників та суб'єктів розгортання певних систем ШІ

Розділ V — ШІ загального призначення

Ст. 51 · Класифікація загальноцільових моделей ШІ як загальноцільових моделей ШІ із системним ризиком

Ст. 52 · Процедура

Ст. 53 · Зобов'язання для постачальників загальноцільових моделей ШІ

Ст. 54 · Уповноважені представники постачальників загальноцільових моделей ШІ

Ст. 55 · Зобов'язання постачальників загальноцільових моделей ШІ із системним ризиком

Ст. 56 · Кодекси поведінки

Розділ VI — Заходи підтримки

Ст. 57 · Регуляторні пісочниці зі штучного інтелекту

Ст. 58 · Детальні умови та функціонування регуляторних пісочниць зі штучного інтелекту

Ст. 59 · Подальша обробка персональних даних для розробки певних систем штучного інтелекту в суспільних інтересах у регуляторній пісочниці зі штучного інтелекту

Ст. 60 · Тестування високоризикових систем штучного інтелекту в реальних умовах за межами регуляторних пісочниць зі штучного інтелекту

Ст. 61 · Поінформована згода на участь у тестуванні в реальних умовах за межами регуляторних пісочниць зі штучного інтелекту

Ст. 62 · Заходи для постачальників та суб'єктів розгортання, зокрема МСП, включаючи стартапи

Ст. 63 · Відступи для конкретних операторів

Розділ VII — Управління

Ст. 64 · Офіс зі штучного інтелекту

Ст. 65 · Заснування та структура Європейської ради з питань штучного інтелекту

Ст. 66 · Завдання Ради

Ст. 67 · Консультативний форум

Ст. 68 · Наукова рада незалежних експертів

Ст. 69 · Доступ держав-членів до пулу експертів

Ст. 70 · Призначення національних компетентних органів та єдиних контактних точок

Розділ VIII — База даних ЄС

Ст. 71 · База даних ЄС для високоризикових систем штучного інтелекту, перелічених у Додатку III

Розділ IX — Постринкові вимоги

Ст. 72 · Пост-ринковий моніторинг постачальниками та план пост-ринкового моніторингу для високоризикових систем штучного інтелекту

Ст. 73 · Повідомлення про серйозні інциденти

Ст. 74 · Ринковий нагляд та контроль систем штучного інтелекту на ринку Союзу

Ст. 75 · Взаємна допомога, ринковий нагляд та контроль систем штучного інтелекту загального призначення

Ст. 76 · Нагляд органів ринкового нагляду за тестуванням у реальних умовах

Ст. 77 · Повноваження органів, що захищають основоположні права

Ст. 78 · Конфіденційність

Ст. 79 · Процедура на національному рівні щодо систем штучного інтелекту, що становлять ризик

Ст. 80 · Процедура щодо систем штучного інтелекту, класифікованих постачальником як не-високоризикові при застосуванні Додатку III

Ст. 81 · Захисна процедура Союзу

Ст. 82 · Відповідні системи штучного інтелекту, що становлять ризик

Ст. 83 · Формальна невідповідність

Ст. 84 · Структури підтримки тестування штучного інтелекту Союзу

Ст. 85 · Право на подання скарги до органу ринкового нагляду

Ст. 86 · Право на пояснення при прийнятті індивідуальних рішень

Ст. 87 · Повідомлення про порушення та захист осіб, що повідомляють

Ст. 88 · Застосування зобов'язань постачальників моделей штучного інтелекту загального призначення

Ст. 89 · Дії з моніторингу

Ст. 90 · Оповіщення про системні ризики науковою радою

Ст. 91 · Повноваження щодо запиту документації та інформації

Ст. 92 · Повноваження щодо проведення оцінок

Ст. 93 · Повноваження щодо запиту заходів

Ст. 94 · Процесуальні права суб'єктів господарювання щодо моделі штучного інтелекту загального призначення

Розділ X — Кодекси поведінки

Ст. 95 · Кодекси поведінки для добровільного застосування конкретних вимог

Ст. 96 · Настанови Комісії щодо виконання цього Регламенту

Розділ XI — Делегування повноважень

Ст. 97 · Здійснення делегування

Ст. 98 · Процедура комітету

Розділ XII — Санкції

Ст. 99 · Санкції

Ст. 100 · Адміністративні штрафи для інституцій, органів, служб та агентств Союзу

Ст. 101 · Штрафи для постачальників моделей штучного інтелекту загального призначення

Розділ XIII — Заключні положення

Ст. 102 · Внесення змін до Регламенту (ЄС) № 300/2008

Ст. 103 · Внесення змін до Регламенту (ЄС) № 167/2013

Ст. 104 · Внесення змін до Регламенту (ЄС) № 168/2013

Ст. 105 · Внесення змін до Директиви 2014/90/ЄС

Ст. 106 · Внесення змін до Директиви (ЄС) 2016/797

Ст. 107 · Внесення змін до Регламенту (ЄС) 2018/858

Ст. 108 · Внесення змін до Регламенту (ЄС) 2018/1139

Ст. 109 · Внесення змін до Регламенту (ЄС) 2019/2144

Ст. 110 · Внесення змін до Директиви (ЄС) 2020/1828

Ст. 111 · Системи штучного інтелекту, вже введені в обіг або введені в експлуатацію, та моделі штучного інтелекту загального призначення, вже введені в обіг

Ст. 112 · Оцінка та перегляд

Ст. 113 · Набрання чинності та застосування

Додатки

Додаток I · ДОДАТОК I

Додаток II · ДОДАТОК II

Додаток III · ДОДАТОК III

Додаток IV · ДОДАТОК IV

Додаток V · ДОДАТОК V

Додаток VI · ДОДАТОК VI

Додаток VII · ДОДАТОК VII

Додаток VIII · ДОДАТОК VIII

Додаток IX · ДОДАТОК IX

Додаток X · ДОДАТОК X

Додаток XI · ДОДАТОК XI

Додаток XII · ДОДАТОК XII

Додаток XIII · ДОДАТОК XIII

Повний текст

РЕГЛАМЕНТ (ЄС) 2024/1689 ЄВРОПЕЙСЬКОГО ПАРЛАМЕНТУ І РАДИ

від 13 червня 2024 року

про встановлення гармонізованих правил щодо штучного інтелекту та внесення змін до Регламентів (ЄС) № 300/2008, (ЄС) № 167/2013, (ЄС) № 168/2013, (ЄС) 2018/858, (ЄС) 2018/1139 та (ЄС) 2019/2144 і Директив 2014/90/ЄС, (ЄС) 2016/797 та (ЄС) 2020/1828 (Акт про штучний інтелект)

(Текст стосується ЄЕП)

ЄВРОПЕЙСЬКИЙ ПАРЛАМЕНТ І РАДА ЄВРОПЕЙСЬКОГО СОЮЗУ,

беручи до уваги Договір про функціонування Європейського Союзу, зокрема його статті 16 та 114,

беручи до уваги пропозицію Європейської Комісії,

після передачі проєкту законодавчого акта національним парламентам,

беручи до уваги висновок Європейського економічного та соціального комітету (1),

беручи до уваги висновок Європейського центрального банку (2),

беручи до уваги висновок Комітету регіонів (3),

діючи відповідно до звичайної законодавчої процедури (4),

Тоді як:

(1) Метою цього Регламенту є покращення функціонування внутрішнього ринку шляхом встановлення єдиної правової бази, зокрема для розроблення, виведення на ринок, введення в експлуатацію та використання систем штучного інтелекту (системи ШІ) в Союзі, відповідно до цінностей Союзу, для сприяння впровадженню орієнтованого на людину та заслуговуючого довіри штучного інтелекту (ШІ) при забезпеченні високого рівня захисту здоров'я, безпеки, основоположних прав, закріплених у Хартії основних прав Європейського Союзу (Хартія), включаючи демократію, верховенство права та охорону навколишнього середовища, з метою захисту від шкідливих наслідків систем штучного інтелекту в Союзі та підтримки інновацій. Цей Регламент забезпечує вільне транскордонне переміщення товарів та послуг на основі ШІ, тим самим перешкоджаючи державам-членам запроваджувати обмеження на розроблення, збут та використання систем штучного інтелекту, якщо це прямо не дозволено цим Регламентом.

(2) Цей Регламент має застосовуватися відповідно до цінностей Союзу, закріплених у Хартії, сприяючи захисту фізичних осіб, підприємств, демократії, верховенства права та охорони навколишнього середовища, одночасно стимулюючи інновації та зайнятість і роблячи Союз лідером у впровадженні надійного ШІ.

(3) Системи штучного інтелекту можуть легко впроваджуватись у великій кількості секторів економіки та багатьох сферах суспільства, у тому числі транскордонно, і можуть легко обертатися по всьому Союзу. Деякі держави-члени вже вивчили можливість прийняття національних правил для забезпечення надійності та безпечності ШІ та його розроблення й використання відповідно до зобов'язань у сфері основних прав. Розбіжності в національних правилах можуть призвести до фрагментації внутрішнього ринку та можуть зменшити правову визначеність для суб'єктів, що розробляють, імпортують або використовують системи штучного інтелекту. Тому для досягнення надійного ШІ слід забезпечити послідовний та високий рівень захисту в усьому

Союзі, тоді як розбіжності, що перешкоджають вільному обігу, інноваціям, розгортанню та впровадженню систем штучного інтелекту та пов'язаних продуктів і послуг на внутрішньому ринку, слід запобігти шляхом встановлення єдиних зобов'язань для суб'єктів та гарантування єдиного захисту першочергових підстав публічного інтересу та прав осіб на всьому внутрішньому ринку на підставі статті 114 Договору про функціонування Європейського Союзу (ДФЄС). Тією мірою, якою цей Регламент містить спеціальні правила щодо захисту осіб стосовно обробки персональних даних щодо обмежень використання систем штучного інтелекту для дистанційної біометричної ідентифікації з правоохоронною метою, використання систем штучного інтелекту для оцінки ризиків фізичних осіб з правоохоронною метою та використання систем штучного інтелекту для біометричної категоризації з правоохоронною метою, доцільно базувати цей Регламент, оскільки ці спеціальні правила стосуються, на статті 16 ДФЄС. З огляду на ці спеціальні правила та звернення до статті 16 ДФЄС, доцільно проконсультуватися з Європейською радою захисту даних.

(4) ШІ — це сімейство технологій, що швидко розвивається, яке сприяє широкому спектру економічних, екологічних та суспільних переваг у всьому спектрі галузей і соціальної діяльності. Завдяки вдосконаленню прогнозування, оптимізації операцій та розподілу ресурсів, а також персоналізації цифрових рішень, доступних для фізичних осіб та організацій, використання ШІ може надати підприємствам ключові конкурентні переваги та підтримати соціально та екологічно корисні результати, наприклад, в охороні здоров'я, сільському господарстві, безпечності харчових продуктів, освіті та навчанні, засобах масової інформації, спорті, культурі, управлінні інфраструктурою, енергетиці, транспорті та логістиці, публічних послугах, безпеці, правосудді, ресурсній та енергетичній ефективності, екологічному моніторингу, збереженні та відновленні

біорізноманіття та екосистем, а також пом'якшенні наслідків зміни клімату та адаптації до них.

(5) Водночас, залежно від обставин конкретного застосування, використання та рівня технологічного розвитку, ШІ може генерувати ризики та завдавати шкоди суспільним інтересам та основоположним правам, що захищаються правом Союзу. Така шкода може бути матеріальною або нематеріальною, включаючи фізичну, психологічну, соціальну або економічну шкоду.

(6) З огляду на значний вплив, який ШІ може мати на суспільство, та необхідність формування довіри, вкрай важливо, щоб ШІ та його регуляторна база розвивалися відповідно до цінностей Союзу, закріплених у статті 2 Договору про Європейський Союз (ДЄС), основоположних прав та свобод, закріплених у Договорах, та відповідно до статті 6 ДЄС — у Хартії. Як передумова, ШІ має бути орієнтованою на людину технологією. Він має служити інструментом для людей, кінцевою метою якого є підвищення добробуту людини.

(7) З метою забезпечення послідовного та високого рівня захисту публічних інтересів щодо здоров'я, безпеки та основоположних прав слід встановити спільні правила для високоризикових систем штучного інтелекту. Ці правила мають відповідати Хартії, бути недискримінаційними та відповідати міжнародним торговельним зобов'язанням Союзу. Вони також мають враховувати Європейську декларацію про цифрові права та принципи для цифрового десятиліття та Керівні принципи етики для надійного ШІ Групи експертів високого рівня з питань штучного інтелекту (AI HLEG).

(8) Тому необхідна правова база Союзу, що встановлює гармонізовані правила щодо ШІ, для сприяння розробленню, використанню та впровадженню ШІ на внутрішньому ринку, яка водночас відповідає високому рівню захисту публічних інтересів, таких як здоров'я та безпека, а також захист основоположних прав, включаючи демократію, верховенство права та

охорону навколишнього середовища, як це визнано та захищено законодавством Союзу. Для досягнення цієї мети слід встановити правила, що регулюють виведення на ринок, введення в експлуатацію та використання певних систем штучного інтелекту, тим самим забезпечуючи безперебійне функціонування внутрішнього ринку та дозволяючи цим системам користуватися принципом вільного переміщення товарів та послуг. Ці правила мають бути чіткими та надійними у захисті основоположних прав, підтримувати нові інноваційні рішення, сприяти розвитку європейської екосистеми державних та приватних суб'єктів, що створюють системи штучного інтелекту відповідно до цінностей Союзу, та розкривати потенціал цифрової трансформації в усіх регіонах Союзу. Встановлюючи ці правила, а також заходи на підтримку інновацій з особливим акцентом на малі та середні підприємства (МСП), включаючи стартапи, цей Регламент підтримує мету просування європейського орієнтованого на людину підходу до ШІ та бути світовим лідером у розробленні безпечного, надійного та етичного ШІ, як зазначено Європейською Радою (5), і забезпечує захист етичних принципів, як це спеціально вимагав Європейський Парламент (6).

(9) Гармонізовані правила щодо введення на ринок, введення в експлуатацію та використання систем ШІ з високим ступенем ризику мають встановлюватися у відповідності з Регламентом (ЄС) № 765/2008 Європейського Парламенту і Ради (7), Рішенням № 768/2008/ЄС Європейського Парламенту і Ради (8) та Регламентом (ЄС) 2019/1020 Європейського Парламенту і Ради (9) (Новий законодавчий каркас). Гармонізовані правила, встановлені цим Регламентом, мають застосовуватися в різних секторах і, відповідно до Нового законодавчого каркаса, не повинні порушувати чинне право Союзу, зокрема у сферах захисту даних, захисту прав споживачів, основоположних прав, зайнятості та захисту працівників і безпечності продукції, яке цей Регламент доповнює. Отже, всі права та засоби правового захисту, передбачені таким правом Союзу для споживачів та інших осіб, на яких системи ШІ можуть негативно

впливати, включаючи відшкодування можливої шкоди згідно з Директивою Ради 85/374/ЄЕС (10) залишаються незміненими та повністю застосовними. Крім того, у контексті зайнятості та захисту працівників цей Регламент не повинен впливати на право Союзу у сфері соціальної політики та на національне трудове право, що відповідає праву Союзу, стосовно умов зайнятості та праці, включаючи охорону здоров'я та безпеку на виробництві, а також відносини між роботодавцями та працівниками. Цей Регламент також не повинен впливати на реалізацію основоположних прав, визнаних у державах-членах та на рівні Союзу, включаючи право або свободу страйкувати чи вживати інших заходів, передбачених конкретними системами трудових відносин у державах-членах, а також право вести переговори, укладати та виконувати колективні договори або вживати колективних заходів відповідно до національного законодавства. Цей Регламент не повинен стосуватися положень, спрямованих на покращення умов праці у платформній зайнятості, встановлених Директивою Європейського Парламенту і Ради про покращення умов праці у платформній зайнятості. Більше того, цей Регламент прагне посилити ефективність таких існуючих прав та засобів правового захисту шляхом встановлення конкретних вимог та зобов'язань, у тому числі щодо прозорості, технічної документації та ведення обліку систем ШІ. Крім того, зобов'язання, що покладаються цим Регламентом на різних операторів, задіяних у ланцюгу цінності ШІ, мають застосовуватися без шкоди для національного законодавства, що відповідає праву Союзу, яке обмежує використання певних систем ШІ, якщо таке законодавство виходить за межі сфери застосування цього Регламенту або переслідує законні цілі в сфері суспільних інтересів, відмінні від тих, що переслідуються цим Регламентом. Наприклад, національне трудове законодавство та законодавство про захист неповнолітніх, тобто осіб, молодших 18 років, з урахуванням Загального коментаря № 25 (2021) Комітету ООН з прав дитини щодо прав дітей у цифровому середовищі, оскільки вони не

є специфічними для систем ШІ та переслідують інші законні цілі суспільного інтересу, не повинні зазнавати впливу цього Регламенту.

(10) Основоположне право на захист персональних даних забезпечується зокрема Регламентами (ЄС) 2016/679 (11) та (ЄС) 2018/1725 (12) Європейського Парламенту і Ради та Директивою (ЄС) 2016/680 Європейського Парламенту і Ради (13). Директива 2002/58/ЄС Європейського Парламенту і Ради (14) додатково захищає приватне життя та конфіденційність комунікацій, у тому числі шляхом встановлення умов будь-якого зберігання персональних і неперсональних даних у кінцевому обладнанні та доступу до них з нього. Ці правові акти Союзу забезпечують основу для стійкої та відповідальної обробки даних, включаючи випадки, коли набори даних містять суміш персональних і неперсональних даних. Цей Регламент не прагне вплинути на застосування чинного права Союзу, що регулює обробку персональних даних, включаючи завдання та повноваження незалежних наглядових органів, компетентних здійснювати нагляд за дотриманням цих інструментів. Він також не стосується зобов'язань постачальників та операторів систем ШІ у їх ролі контролерів або обробників даних, що випливають із права Союзу або національного законодавства про захист персональних даних, оскільки проєктування, розробка або використання систем ШІ пов'язані з обробкою персональних даних. Також доцільно уточнити, що суб'єкти даних продовжують користуватися всіма правами та гарантіями, наданими їм таким правом Союзу, включаючи права, пов'язані виключно з автоматизованим індивідуальним прийняттям рішень, у тому числі профілюванням. Гармонізовані правила щодо введення на ринок, введення в експлуатацію та використання систем ШІ, встановлені цим Регламентом, мають сприяти ефективному виконанню та забезпечувати реалізацію прав суб'єктів даних та інших засобів правового захисту, гарантованих правом Союзу про захист персональних даних та інших основоположних прав.

(11) Цей Регламент не повинен порушувати положення щодо відповідальності постачальників посередницьких послуг, викладені в Регламенті (ЄС) 2022/2065 Європейського Парламенту і Ради (15).

(12) Поняття «система ШІ» в цьому Регламенті має бути чітко визначене та тісно узгоджене з роботою міжнародних організацій, що займаються питаннями ШІ, для забезпечення правової визначеності, сприяння міжнародному зближенню та широкого визнання, при цьому зберігаючи гнучкість для врахування стрімких технологічних змін у цій сфері. Крім того, визначення має ґрунтуватися на ключових характеристиках систем ШІ, що відрізняють їх від простіших традиційних програмних систем або підходів до програмування, і не повинно охоплювати системи, що базуються виключно на правилах, визначених фізичними особами для автоматичного виконання операцій. Ключовою характеристикою систем ШІ є їхня здатність робити висновки. Ця здатність робити висновки означає процес отримання результатів, таких як прогнози, контент, рекомендації або рішення, що можуть впливати на фізичні та віртуальні середовища, а також здатність систем ШІ виводити моделі або алгоритми, або те й інше, на основі вхідних даних або даних. Методи, що уможливлюють виведення при побудові системи ШІ, включають підходи машинного навчання, що дозволяють навчатися за даними для досягнення певних цілей, а також підходи на основі логіки та знань, що виводять результати із закодованих знань або символічного представлення задачі, яку потрібно вирішити. Здатність системи ШІ робити висновки виходить за межі базової обробки даних, уможливлюючи навчання, міркування або моделювання. Термін «машинно-орієнтований» означає, що системи ШІ функціонують на машинах. Посилання на явні або неявні цілі підкреслює, що системи ШІ можуть функціонувати відповідно до явно визначених або неявних цілей. Цілі системи ШІ можуть відрізнятися від передбачуваного призначення системи ШІ в конкретному контексті. Для цілей цього Регламенту під середовищами слід розуміти контексти, в яких

функціонують системи ШІ, тоді як результати, генеровані системою ШІ, відображають різні функції, що виконуються системами ШІ, та включають прогнози, контент, рекомендації або рішення. Системи ШІ призначені для роботи з різними рівнями автономності, тобто вони мають певний ступінь незалежності дій від участі людини та здатності функціонувати без втручання людини. Адаптивність, яку система ШІ може виявляти після розгортання, означає здатність до самонавчання, що дозволяє системі змінюватися під час використання. Системи ШІ можуть використовуватися самостійно або як компонент продукту, незалежно від того, чи система фізично інтегрована у продукт (вбудована), чи забезпечує функціональність продукту, не будучи в нього інтегрованою (невбудована).

(13) Поняття «оператор», що вживається в цьому Регламенті, слід тлумачити як будь-яку фізичну або юридичну особу, включаючи органи публічної влади, агентства або інші органи, що використовують систему ШІ під своїм керівництвом, за винятком випадків, коли система ШІ використовується в процесі особистої непрофесійної діяльності. Залежно від типу системи ШІ її використання може стосуватися осіб, відмінних від оператора.

(14) Поняття «біометричні дані», що вживається в цьому Регламенті, слід тлумачити у світлі поняття біометричних даних, визначеного у статті 4, пункт (14) Регламенту (ЄС) 2016/679, статті 3, пункт (18) Регламенту (ЄС) 2018/1725 та статті 3, пункт (13) Директиви (ЄС) 2016/680. Біометричні дані можуть дозволяти автентифікацію, ідентифікацію або категоризацію фізичних осіб, а також розпізнавання емоцій фізичних осіб.

(15) Поняття «біометрична ідентифікація», що вживається в цьому Регламенті, має визначатися як автоматичне розпізнавання фізичних, фізіологічних та поведінкових характеристик людини, таких як обличчя, рух очей, форма тіла, голос, просодія, хода, поза, частота серцевих скорочень, артеріальний тиск, запах, характеристики натискання клавіш, з метою

встановлення особи індивіда шляхом порівняння біометричних даних цього індивіда зі збереженими біометричними даними осіб у референтній базі даних, незалежно від того, чи надав індивід свою згоду. Це виключає системи ШІ, призначені для біометричної верифікації, яка включає автентифікацію, єдиною метою якої є підтвердження того, що конкретна фізична особа є тією, за яку себе видає, та підтвердження особи фізичної особи виключно з метою отримання доступу до послуги, розблокування пристрою або отримання охоронного доступу до приміщень.

(16) Поняття «біометрична категоризація», що вживається в цьому Регламенті, має визначатися як віднесення фізичних осіб до конкретних категорій на основі їхніх біометричних даних. Такі конкретні категорії можуть стосуватися аспектів, таких як стать, вік, колір волосся, колір очей, татуювання, поведінкові або особистісні риси, мова, релігія, приналежність до національної меншини, сексуальна або політична орієнтація. Це не включає системи біометричної категоризації, що є суто допоміжною функцією, нерозривно пов'язаною з іншою комерційною послугою, тобто функція, яка з об'єктивних технічних причин не може використовуватися без основної послуги, а інтеграція такої функції або функціональності не є засобом обходу застосовуваності норм цього Регламенту. Наприклад, фільтри, що категоризують риси обличчя або тіла, що використовуються на онлайн-ринках, можуть становити таку допоміжну функцію, оскільки вони можуть використовуватися лише у зв'язку з основною послугою, що полягає у продажу товару, дозволяючи споживачеві попередньо переглянути відображення товару на собі та допомогти споживачеві прийняти рішення про покупку. Фільтри, що використовуються в онлайн-сервісах соціальних мереж і категоризують риси обличчя або тіла, щоб дозволити користувачам додавати або змінювати зображення чи відео, також можуть вважатися допоміжною функцією, оскільки такий фільтр не

може використовуватися без основної послуги сервісів соціальних мереж, що полягає у поширенні контенту онлайн.

(17) Поняття «система дистанційної біометричної ідентифікації», що вживається в цьому Регламенті, має визначатися функціонально як система ШІ, призначена для ідентифікації фізичних осіб без їхньої активної участі, як правило, на відстані, шляхом порівняння біометричних даних особи з біометричними даними, що містяться в референтній базі даних, незалежно від конкретної технології, процесів або типів використовуваних біометричних даних. Такі системи дистанційної біометричної ідентифікації, як правило, використовуються для одночасного сприйняття кількох осіб або їхньої поведінки з метою суттєвого полегшення ідентифікації фізичних осіб без їхньої активної участі. Це виключає системи ШІ, призначені для біометричної верифікації, яка включає автентифікацію, єдиною метою якої є підтвердження того, що конкретна фізична особа є тією, за яку себе видає, та підтвердження особи фізичної особи виключно з метою отримання доступу до послуги, розблокування пристрою або отримання охоронного доступу до приміщень. Таке виключення виправдане тим, що такі системи, ймовірно, матимуть незначний вплив на основоположні права фізичних осіб порівняно з системами дистанційної біометричної ідентифікації, які можуть використовуватися для обробки біометричних даних великої кількості осіб без їхньої активної участі. У випадку систем «реального часу» захоплення біометричних даних, порівняння та ідентифікація відбуваються миттєво, майже миттєво або в будь-якому разі без значної затримки. У цьому відношенні не повинно бути можливості обходу норм цього Регламенту щодо використання «в реальному часі» відповідних систем ШІ шляхом передбачення незначних затримок. Системи «реального часу» передбачають використання матеріалів «в прямому ефірі» або «майже в прямому ефірі», таких як відеозаписи, що генеруються камерою або іншим пристроєм з аналогічною функціональністю. У випадку «постсистем», навпаки, біометричні дані вже

захоплені, а порівняння та ідентифікація відбуваються лише після значної затримки. Це передбачає матеріали, такі як фотографії або відеозаписи, що генеруються камерами відеоспостереження або приватними пристроями, які були отримані до використання системи стосовно відповідних фізичних осіб.

(18) Поняття «система розпізнавання емоцій», що вживається в цьому Регламенті, має визначатися як система ШІ з метою ідентифікації або виведення емоцій чи намірів фізичних осіб на основі їхніх біометричних даних. Це поняття охоплює такі емоції або наміри, як радість, смуток, гнів, подив, огида, збентеження, збудження, сором, презирство, задоволення та розвага. Воно не включає фізичні стани, такі як біль або втома, включаючи, наприклад, системи, що використовуються для виявлення стану втоми у пілотів-професіоналів або водіїв з метою запобігання нещасним випадкам. Воно також не включає просте виявлення явно виражених виразів обличчя, жестів або рухів, якщо вони не використовуються для ідентифікації або виведення емоцій. Такими виразами можуть бути базові вирази обличчя, такі як насуплений лоб або посмішка, або жести, такі як рух рук, рук або голови, або характеристики голосу людини, такі як підвищений голос або шепіт.

(19) Для цілей цього Регламенту поняття «загальнодоступний простір» слід розуміти як посилання на будь-який фізичний простір, доступний для невизначеної кількості фізичних осіб, незалежно від того, чи є відповідний простір приватним або публічним, незалежно від діяльності, для якої він може використовуватися, наприклад для торгівлі — магазини, ресторани, кафе; для послуг — банки, професійна діяльність, готельний бізнес; для спорту — плавальні басейни, спортивні зали, стадіони; для транспорту — автобусні, метро- та залізничні станції, аеропорти, транспортні засоби; для розваг — кінотеатри, театри, музеї, концертні та конференц-зали; або для дозвілля чи інших цілей — громадські дороги та площі, парки, ліси, ігрові майданчики. Простір також слід класифікувати як загальнодоступний, якщо

незалежно від можливих обмежень щодо місткості або безпеки доступ до нього підпорядковується певним заздалегідь визначеним умовам, які може виконати невизначена кількість осіб, наприклад придбання квитка або проїзного документа, попередня реєстрація або досягнення певного віку. Навпаки, простір не слід вважати загальнодоступним, якщо доступ до нього обмежений конкретними та визначеними фізичними особами відповідно до права Союзу або національного права, безпосередньо пов'язаного з публічною безпекою або охороною, або шляхом явного виявлення волі особою, що має відповідні повноваження щодо цього простору. Лише фактична можливість доступу, наприклад незамкнені двері або відкрита хвіртка в огорожі, не означає, що простір є загальнодоступним за наявності ознак або обставин, що свідчать про протилежне, наприклад знаків, що забороняють або обмежують доступ. Приміщення підприємств і заводів, а також офіси та робочі місця, до яких призначений доступ лише для відповідних працівників і постачальників послуг, є просторами, що не є загальнодоступними. Загальнодоступні простори не повинні включати в'язниці або прикордонний контроль. Деякі інші простори можуть включати як загальнодоступні, так і незагальнодоступні простори, наприклад вестибюль приватного житлового будинку, необхідного для доступу до лікарського кабінету або аеропорту. Онлайн-простори не охоплюються, оскільки вони не є фізичними просторами. Однак питання про те, чи є певний простір загальнодоступним, слід вирішувати в кожному конкретному випадку, з урахуванням особливостей конкретної ситуації.

(20) З метою отримання максимальної користі від систем ШІ при захисті основоположних прав, здоров'я та безпеки, а також для забезпечення демократичного контролю, грамотність у сфері ШІ має забезпечувати постачальників, операторів та осіб, яких це стосується, необхідними знаннями для прийняття обґрунтованих рішень щодо систем ШІ. Такі знання можуть відрізнятися залежно від відповідного контексту та можуть включати

розуміння правильного застосування технічних елементів на етапі розробки системи ШІ, заходів, що мають застосовуватися під час її використання, відповідних способів інтерпретації результатів системи ШІ, а у випадку осіб, яких це стосується, — знань, необхідних для розуміння того, який вплив матимуть на них рішення, прийняті за допомогою ШІ. У контексті застосування цього Регламенту грамотність у сфері ШІ має надавати всім відповідним суб'єктам у ланцюгу цінності ШІ уявлення, необхідні для забезпечення належного дотримання вимог та їх правильного виконання. Крім того, широке впровадження заходів з підвищення грамотності у сфері ШІ та запровадження відповідних подальших дій можуть сприяти покращенню умов праці та зрештою підтримати консолідацію та інноваційний шлях надійного ШІ в Союзі. Рада з питань штучного інтелекту (далі — «Рада») має підтримувати Комісію в просуванні інструментів грамотності у сфері ШІ, суспільної обізнаності та розуміння переваг, ризиків, захисних заходів, прав та обов'язків у зв'язку з використанням систем ШІ. У співпраці з відповідними зацікавленими сторонами Комісія та держави-члени мають сприяти розробці добровільних кодексів поведінки для підвищення грамотності у сфері ШІ серед осіб, що займаються розробкою, експлуатацією та використанням ШІ.

(21) З метою забезпечення рівних умов гри та ефективного захисту прав і свобод осіб на всій території Союзу правила, встановлені цим Регламентом, мають застосовуватися до постачальників систем ШІ на недискримінаційній основі, незалежно від того, чи вони засновані в межах Союзу або в третій країні, а також до операторів систем ШІ, засновані в межах Союзу.

(22) З огляду на їхній цифровий характер, певні системи ШІ мають підпадати під сферу застосування цього Регламенту, навіть якщо вони не введені на ринок, не введені в експлуатацію або не використовуються в Союзі. Це стосується, наприклад, випадків, коли оператор, заснований у Союзі, укладає договір на певні послуги з

оператором, заснованим у третій країні, у зв'язку з діяльністю, яку має виконувати система ШІ, що відповідатиме критеріям систем з високим ступенем ризику. За таких обставин система ШІ, що використовується в третій країні оператором, може обробляти законно зібрані в Союзі та передані з нього дані та надавати оператору-замовнику в Союзі результат цієї системи ШІ від такої обробки, не будучи введеною на ринок, в експлуатацію або використаною в Союзі. Для запобігання обходу цього Регламенту та забезпечення ефективного захисту фізичних осіб, що знаходяться в Союзі, цей Регламент також має застосовуватися до постачальників та операторів систем ШІ, заснованих у третій країні, в тій мірі, в якій результат, що виробляється цими системами, призначений для використання в Союзі. Тим не менш, з урахуванням існуючих домовленостей та особливих потреб для майбутньої співпраці із закордонними партнерами, з якими обмінюються інформацією та доказами, цей Регламент не повинен застосовуватися до органів публічної влади третіх країн та міжнародних організацій, що діють у рамках угод про співпрацю або міжнародних угод, укладених на рівні Союзу або держав-членів для правоохоронної та судової співпраці з Союзом або державами-членами, за умови, що відповідна третя країна або міжнародна організація надає належні гарантії щодо захисту основоположних прав і свобод осіб. Там, де це доречно, це може охоплювати діяльність суб'єктів, яким треті країни доручили виконання конкретних завдань на підтримку такої правоохоронної та судової співпраці. Такі рамки для співпраці або угоди були встановлені двосторонньо між державами-членами та третіми країнами або між Європейським Союзом, Європолом та іншими агентствами Союзу і третіми країнами та міжнародними організаціями. Органи, компетентні для нагляду за правоохоронними та судовими органами відповідно до цього Регламенту, мають оцінювати, чи включають ці рамки для співпраці або міжнародні угоди належні гарантії щодо захисту основоположних прав і свобод осіб. Національні органи-одержувачі та інститути, органи, служби та агентства Союзу, що

використовують такі результати в Союзі, залишаються відповідальними за забезпечення того, щоб їх використання відповідало праву Союзу. Коли ці міжнародні угоди переглядаються або в майбутньому укладаються нові, сторони, що домовляються, мають докладати максимальних зусиль для приведення цих угод у відповідність до вимог цього Регламенту.

(23) Цей Регламент також має застосовуватися до інститутів, органів, служб та агентств Союзу, коли вони виступають як постачальник або оператор системи ШІ.

(24) Якщо та настільки, наскільки системи ШІ вводяться на ринок, вводяться в експлуатацію або використовуються з модифікацією або без неї таких систем для військових, оборонних або цілей національної безпеки, вони мають виключатися зі сфери застосування цього Регламенту незалежно від того, який тип суб'єкта здійснює ці заходи, наприклад чи є він публічним або приватним суб'єктом. Щодо військових та оборонних цілей, таке виключення обґрунтовується як статтею 4(2) ДЄС, так і особливостями спільної оборонної політики держав-членів та Союзу, що охоплюється главою 2 розділу V ДЄС, яка регулюється міжнародним публічним правом, що є тому більш відповідною правовою базою для регулювання систем ШІ у контексті застосування летальної сили та інших систем ШІ у контексті військової та оборонної діяльності. Щодо цілей національної безпеки, виключення обґрунтовується як тим, що національна безпека залишається виключною відповідальністю держав-членів відповідно до статті 4(2) ДЄС, так і конкретним характером та операційними потребами діяльності у сфері національної безпеки, а також конкретними національними нормами, що застосовуються до такої діяльності. Тим не менш, якщо система ШІ, розроблена, введена на ринок, введена в експлуатацію або використана для військових, оборонних або цілей національної безпеки, тимчасово або постійно використовується поза цими цілями для інших цілей, наприклад для цивільних або гуманітарних цілей, правоохоронних або цілей публічної безпеки,

така система підпадатиме під сферу застосування цього Регламенту. У такому разі суб'єкт, що використовує систему ШІ для цілей, відмінних від військових, оборонних або цілей національної безпеки, має забезпечувати відповідність системи ШІ цьому Регламенту, якщо система вже не відповідає цьому Регламенту. Системи ШІ, введені на ринок або введені в експлуатацію для виключеної мети, а саме для військових, оборонних або цілей національної безпеки, та однієї або кількох невиключених цілей, таких як цивільні цілі або правоохоронна діяльність, підпадають під сферу застосування цього Регламенту, і постачальники таких систем мають забезпечувати відповідність цьому Регламенту. У таких випадках той факт, що система ШІ може підпадати під сферу застосування цього Регламенту, не повинен впливати на можливість суб'єктів, що здійснюють діяльність у сфері національної безпеки, оборони та військовій сфері, незалежно від типу суб'єкта, що здійснює цю діяльність, використовувати системи ШІ для цілей національної безпеки, військових та оборонних цілей, використання яких виключено зі сфери застосування цього Регламенту. Система ШІ, введена на ринок для цивільних або правоохоронних цілей, що використовується з модифікацією або без неї для військових, оборонних або цілей національної безпеки, не повинна підпадати під сферу застосування цього Регламенту, незалежно від типу суб'єкта, що здійснює ці заходи.

(25) Цей Регламент має підтримувати інновації, поважати свободу науки та не підривати науково-дослідну та дослідно-конструкторську діяльність. Тому необхідно виключити зі сфери його застосування системи та моделі ШІ, розроблені та введені в експлуатацію спеціально з єдиною метою наукових досліджень і розробок. Крім того, необхідно забезпечити, щоб цей Регламент жодним іншим чином не впливав на науково-дослідну та дослідно-конструкторську діяльність щодо систем або моделей ШІ до їх введення на ринок або введення в експлуатацію. Щодо продуктово-орієнтованої дослідницької, випробувальної та розробницької діяльності щодо систем або моделей ШІ, положення цього

Регламенту також не мають застосовуватися до введення цих систем та моделей в експлуатацію або на ринок. Таке виключення не порушує зобов'язання дотримуватися цього Регламенту, якщо система ШІ, що підпадає під сферу застосування цього Регламенту, вводиться на ринок або в експлуатацію в результаті такої науково-дослідної та дослідно-конструкторської діяльності, та застосування положень про регуляторні пісочниці ШІ та випробування в реальних умовах. Крім того, без шкоди для виключення систем ШІ, розроблених та введених в експлуатацію спеціально з єдиною метою наукових досліджень і розробок, будь-яка інша система ШІ, що може використовуватися для проведення будь-якої науково-дослідної та дослідно-конструкторської діяльності, має залишатися предметом положень цього Регламенту. У будь-якому разі будь-яка науково-дослідна та дослідно-конструкторська діяльність має здійснюватися відповідно до визнаних етичних і професійних стандартів наукових досліджень і проводитися відповідно до застосовного права Союзу.

(26) З метою запровадження пропорційного та ефективного набору обов'язкових правил для систем ШІ необхідно дотримуватися чітко визначеного підходу, заснованого на оцінці ризиків. Такий підхід має адаптувати вид і зміст таких правил до інтенсивності та обсягу ризиків, які можуть генерувати системи ШІ. Тому необхідно забороняти певні неприйнятні практики ШІ, встановлювати вимоги до систем ШІ з високим ступенем ризику та зобов'язання для відповідних операторів, а також встановлювати зобов'язання щодо прозорості для певних систем ШІ.

(27) Хоча підхід, заснований на оцінці ризиків, є основою для пропорційного та ефективного набору обов'язкових правил, важливо нагадати Керівні принципи щодо етики надійного ШІ 2019 року, розроблені незалежною Групою експертів високого рівня з питань ШІ (AI HLEG), призначеною Комісією. У цих керівних принципах AI HLEG розробила сім необов'язкових етичних принципів для ШІ, які

покликані допомогти забезпечити надійність та етичність ШІ. Сім принципів включають: людську свободу дій та нагляд; технічну стійкість та безпеку; приватність та управління даними; прозорість; різноманітність, недискримінацію та справедливість; добробут суспільства та навколишнього середовища; та підзвітність. Без шкоди для юридично обов'язкових вимог цього Регламенту та будь-якого іншого застосовного права Союзу, ці керівні принципи сприяють розробці узгодженого, надійного та антропоцентричного ШІ відповідно до Хартії та цінностей, на яких заснований Союз. Відповідно до керівних принципів AI HLEG, людська свобода дій та нагляд означає, що системи ШІ розробляються та використовуються як інструмент, що служить людям, поважає людську гідність та особисту автономію, і функціонує таким чином, що може належним чином контролюватися людьми. Технічна стійкість та безпека означає, що системи ШІ розробляються та використовуються таким чином, що дозволяє стійкість у разі проблем і стійкість до спроб змінити використання або продуктивність системи ШІ, щоб дозволити незаконне використання третіми сторонами, та мінімізувати ненавмисну шкоду. Приватність та управління даними означає, що системи ШІ розробляються та використовуються відповідно до правил конфіденційності та захисту даних при обробці даних, що відповідають високим стандартам якості та цілісності. Прозорість означає, що системи ШІ розробляються та використовуються таким чином, що дозволяє відповідне відстеження та пояснюваність, водночас інформуючи людей про те, що вони спілкуються або взаємодіють із системою ШІ, а також належним чином інформуючи операторів про можливості та обмеження цієї системи ШІ та осіб, яких це стосується, про їхні права. Різноманітність, недискримінація та справедливість означає, що системи ШІ розробляються та використовуються таким чином, що включає різноманітних суб'єктів та сприяє рівному доступу, гендерній рівності та культурному різноманіттю, уникаючи дискримінаційних наслідків та несправедливих упереджень, що заборонені правом Союзу або

національним законодавством. Добробут суспільства та навколишнього середовища означає, що системи ШІ розробляються та використовуються стійким та екологічно безпечним чином, а також таким чином, щоб приносити користь усім людям, відстежуючи та оцінюючи довгострокові наслідки для особи, суспільства та демократії. Застосування цих принципів має, по можливості, відображатися у проєктуванні та використанні моделей ШІ. Вони у будь-якому разі мають слугувати основою для розробки кодексів поведінки відповідно до цього Регламенту. Усіх зацікавлених сторін, у тому числі промисловість, наукові кола, громадянське суспільство та організації зі стандартизації, заохочують враховувати, за потреби, етичні принципи для розробки добровільних передових практик та стандартів.

(28) Поряд із численними корисними сферами застосування ШІ, він може також зловживатися та надавати нові та потужні інструменти для маніпулятивних, експлуататорських та практик соціального контролю. Такі практики є особливо шкідливими та образливими і мають бути заборонені, оскільки вони суперечать цінностям Союзу — повазі до людської гідності, свободи, рівності, демократії та верховенства права, а також основоположним правам, закріпленим у Хартії, включаючи право на недискримінацію, захист даних та приватність, а також права дитини.

(29) Маніпулятивні технології на основі ШІ можуть використовуватися для переконання осіб у небажаній поведінці або для введення їх в оману шляхом підштовхування до рішень у спосіб, що підриває та обмежує їхню автономію, прийняття рішень і вільний вибір. Введення на ринок, введення в експлуатацію або використання певних систем ШІ з метою або наслідком суттєвого викривлення поведінки людини, при якому ймовірне заподіяння значної шкоди, зокрема досить істотний несприятливий вплив на фізичне, психологічне здоров'я або фінансові інтереси, є особливо небезпечним і тому має бути заборонено. Такі системи ШІ використовують підсвідомі компоненти, такі як аудіо-, фото-,

відеостимули, що не можуть бути сприйняті особами, оскільки ці стимули є поза межами сприйняття людини, або інші маніпулятивні або оманливі прийоми, що підривають або обмежують автономію, прийняття рішень або вільний вибір особи таким чином, що люди не усвідомлено обізнані про ці прийоми, або де вони обізнані про них, можуть все ж бути введені в оману або не здатні контролювати їх або чинити їм опір. Цьому може сприяти, наприклад, машинно-мозкові інтерфейси або віртуальна реальність, оскільки вони дозволяють більш високий ступінь контролю над тим, які стимули представляються особам, оскільки вони можуть суттєво викривляти їхню поведінку у значно шкідливий спосіб. Крім того, системи ШІ також можуть іншим чином експлуатувати вразливості особи або конкретної групи осіб через їх вік, інвалідність у значенні Директиви (ЄС) 2019/882 Європейського Парламенту і Ради (16), або конкретну соціальну чи економічну ситуацію, яка, ймовірно, робить цих осіб більш вразливими до експлуатації, наприклад осіб, що живуть у крайній бідності, представників етнічних або релігійних меншин. Такі системи ШІ можуть вводитися на ринок, вводитися в експлуатацію або використовуватися з метою або наслідком суттєвого викривлення поведінки особи таким чином, що спричиняє або розумно ймовірно спричинить значну шкоду цій чи іншій особі або групам осіб, включаючи шкоду, що може накопичуватися з часом, і тому має бути заборонено. Може бути неможливо припускати наявність наміру викривити поведінку, якщо викривлення є результатом зовнішніх щодо системи ШІ факторів, що знаходяться поза контролем постачальника або оператора, а саме факторів, які можуть бути нерозумно передбачуваними і, отже, неможливими для пом'якшення постачальником або оператором системи ШІ. У будь-якому разі немає необхідності, щоб постачальник або оператор мали намір заподіяти значну шкоду, за умови, що така шкода є результатом маніпулятивних або експлуататорських практик на основі ШІ. Заборони на такі практики ШІ доповнюють положення, що містяться в Директиві 2005/29/ЄС Європейського Парламенту і Ради (17),

зокрема несправедливі комерційні практики, що призводять до економічної або фінансової шкоди для споживачів, забороняються за будь-яких обставин, незалежно від того, чи реалізуються вони через системи ШІ чи іншим чином. Заборони маніпулятивних та експлуататорських практик у цьому Регламенті не повинні стосуватися законних практик у контексті медичного лікування, такого як психологічне лікування психічного захворювання або фізична реабілітація, якщо ці практики здійснюються відповідно до застосовного законодавства та медичних стандартів, наприклад явної згоди осіб або їхніх законних представників. Крім того, поширені та законні комерційні практики, наприклад у сфері реклами, що відповідають застосовному законодавству, не повинні самі по собі вважатися шкідливими маніпулятивними практиками на основі ШІ.

(30) Системи біометричної категоризації, що базуються на біометричних даних фізичних осіб, таких як обличчя або відбиток пальця конкретної особи, для виведення або розкриття політичних поглядів, членства в профспілці, релігійних або філософських переконань, раси, статевого життя або сексуальної орієнтації особи, мають бути заборонені. Ця заборона не повинна поширюватися на законне маркування, фільтрацію або категоризацію наборів біометричних даних, отриманих відповідно до права Союзу або національного законодавства, відповідно до біометричних даних, таких як сортування зображень за кольором волосся або кольором очей, що може, наприклад, використовуватися у сфері правоохоронної діяльності.

(31) Системи ШІ, що здійснюють соціальне скорингування фізичних осіб публічними або приватними суб'єктами, можуть призводити до дискримінаційних результатів та виключення певних груп. Вони можуть порушувати право на гідність та недискримінацію, а також цінності рівності та справедливості. Такі системи ШІ оцінюють або класифікують фізичних осіб чи їхні групи на основі численних точок даних, пов'язаних із їхньою соціальною поведінкою в

різних контекстах або відомими, виведеними чи передбаченими особистісними характеристиками протягом певних проміжків часу. Соціальний рейтинг, отриманий від таких систем ШІ, може призводити до шкідливого або несприятливого поводження з фізичними особами чи цілими їхніми групами в соціальних контекстах, не пов'язаних із контекстом, у якому дані первісно створювалися або збиралися, або до шкідливого поводження, непропорційного або невиправданого тяжкістю їхньої соціальної поведінки. Системи ШІ, що передбачають такі неприйнятні практики скорингування та призводять до таких шкідливих або несприятливих наслідків, мають тому бути заборонені. Ця заборона не повинна стосуватися законних практик оцінки фізичних осіб, що здійснюються для конкретної мети відповідно до права Союзу та національного права.

(32) Використання систем ШІ для дистанційної біометричної ідентифікації фізичних осіб у режимі реального часу в загальнодоступних просторах з метою правоохоронної діяльності є особливо інтрузивним щодо прав і свобод відповідних осіб, тою мірою, якою це може впливати на приватне життя значної частини населення, породжувати відчуття постійного стеження та опосередковано стримувати здійснення свободи зібрань та інших основоположних прав. Технічні неточності систем ШІ, призначених для дистанційної біометричної ідентифікації фізичних осіб, можуть призводити до упереджених результатів і тягнути за собою дискримінаційні наслідки. Такі можливі упереджені результати та дискримінаційні наслідки є особливо актуальними стосовно віку, етнічного походження, раси, статі або інвалідності. Крім того, безпосередність впливу та обмежені можливості для подальших перевірок або виправлень стосовно використання таких систем, що функціонують у режимі реального часу, несуть підвищені ризики для прав і свобод відповідних осіб у контексті правоохоронної діяльності або під її впливом.

(33)

Використання таких систем у цілях правоохоронної діяльності має тому бути заборонено, за винятком вичерпно перелічених і вузько визначених ситуацій, коли використання є суворо необхідним для досягнення суттєвого суспільного інтересу, важливість якого переважує ризики. Такі ситуації охоплюють пошук певних жертв злочинів, у тому числі зниклих безвісти осіб; певні загрози життю або фізичній безпеці фізичних осіб або загрозу терористичного нападу; а також встановлення місцезнаходження або ідентифікацію виконавців або підозрюваних у кримінальних правопорушеннях, перелічених у додатку до цього Регламенту, де такі кримінальні правопорушення карані у відповідній державі-члені позбавленням волі або ухвалою про тримання під вартою на максимальний строк щонайменше чотири роки і відповідно до визначення, передбаченого законодавством тієї держави-члена. Такий поріг для позбавлення волі або ухвали про тримання під вартою відповідно до національного законодавства сприяє забезпеченню того, щоб правопорушення було достатньо серйозним, аби потенційно виправдати використання систем дистанційної біометричної ідентифікації в режимі реального часу. Крім того, перелік кримінальних правопорушень, наведений у додатку до цього Регламенту, ґрунтується на 32 кримінальних правопорушеннях, перелічених у Рамковому рішенні Ради 2002/584/ЄСП (18), беручи до уваги, що деякі з цих правопорушень на практиці, ймовірно, будуть більш актуальними, ніж інші, оскільки звернення до дистанційної біометричної ідентифікації в режимі реального часу могло б, передбачувано, бути необхідним і пропорційним у дуже різній мірі для практичного встановлення місцезнаходження або ідентифікації виконавця чи підозрюваного в різних перелічених кримінальних правопорушеннях з урахуванням ймовірних відмінностей у серйозності, імовірності та масштабах шкоди або можливих негативних наслідків. Безпосередня загроза життю або фізичній безпеці фізичних осіб може також виникнути внаслідок серйозного порушення роботи критичної інфраструктури, як визначено в статті 2, пункт (4) Директиви Європейського

Парламенту і Ради (ЄС) 2022/2557 (19), де порушення або знищення такої критичної інфраструктури спричинило б безпосередню загрозу життю або фізичній безпеці особи, у тому числі через серйозну шкоду забезпеченню населення основними товарами або здійсненню основних функцій держави. Крім того, цей Регламент має зберігати можливість для правоохоронних органів, органів прикордонного контролю, органів у справах міграції або надання притулку здійснювати перевірки документів у присутності відповідної особи відповідно до умов, встановлених правом Союзу та національним законодавством для таких перевірок. Зокрема, правоохоронні органи, органи прикордонного контролю, органи у справах міграції або надання притулку мають мати можливість використовувати інформаційні системи відповідно до права Союзу або національного права для ідентифікації осіб, які під час перевірки документів відмовляються бути ідентифікованими або не в змозі повідомити чи підтвердити свою особу, без обов'язкового отримання попереднього дозволу відповідно до цього Регламенту. Це може бути, наприклад, особа, причетна до злочину, яка не бажає або не здатна через нещасний випадок чи стан здоров'я розкрити свою особу правоохоронним органам.

(34) З метою забезпечення відповідального та пропорційного використання таких систем важливо також встановити, що в кожній із цих вичерпно перелічених і вузько визначених ситуацій мають братися до уваги певні елементи, зокрема щодо характеру ситуації, що дала підставу для запиту, і наслідків використання для прав і свобод усіх відповідних осіб, а також гарантій і умов, передбачених для використання. Крім того, використання систем дистанційної біометричної ідентифікації в режимі реального часу в загальнодоступних просторах у цілях правоохоронної діяльності має застосовуватися лише для підтвердження особи конкретно цільової особи та має обмежуватися суворо необхідним щодо часового проміжку, а також географічного та особистісного охоплення, особливо з урахуванням доказів або ознак щодо загроз, жертв або виконавця. Використання

системи дистанційної біометричної ідентифікації в режимі реального часу в загальнодоступних просторах має бути авторизовано лише за умови, що відповідний правоохоронний орган завершив оцінку впливу на основоположні права і, якщо цим Регламентом не передбачено інше, зареєстрував систему в базі даних, як передбачено цим Регламентом. Довідкова база даних осіб має відповідати кожному варіанту використання в кожній із зазначених вище ситуацій.

(35) Кожне використання системи дистанційної біометричної ідентифікації в режимі реального часу в загальнодоступних просторах у цілях правоохоронної діяльності має бути предметом явного і конкретного дозволу з боку судового органу або незалежного адміністративного органу держави-члена, рішення якого є обов'язковим. Такий дозвіл має, як правило, бути отриманий до використання системи ШІ з метою ідентифікації особи або осіб. Винятки з цього правила мають допускатися у належним чином обґрунтованих ситуаціях з підстав невідкладності, а саме в ситуаціях, коли потреба у використанні відповідних систем є такою, що унеможливлює ефективне та об'єктивне отримання дозволу до початку використання системи ШІ. У таких невідкладних ситуаціях використання системи ШІ має бути обмежено абсолютним мінімумом, необхідним для вирішення завдання, та підпорядковуватися відповідним гарантіям і умовам, визначеним у національному праві та конкретизованим у контексті кожного конкретного невідкладного варіанту використання самим правоохоронним органом. Крім того, у таких ситуаціях правоохоронний орган має запросити такий дозвіл, наводячи підстави неможливості звернення з таким запитом раніше, без невиправданої затримки і не пізніше ніж протягом 24 годин. Якщо такий дозвіл відхиляється, використання систем біометричної ідентифікації в режимі реального часу, пов'язаних із цим дозволом, має негайно припинитися, а всі дані, пов'язані з таким використанням, мають бути відкинуті та видалені. Такі дані включають вхідні дані,

безпосередньо отримані системою ШІ під час використання такої системи, а також результати та вихідні дані використання, пов'язаного з цим дозволом. Вони не мають включати вхідні дані, законно отримані відповідно до іншого права Союзу або національного права. У будь-якому разі жодне рішення, що має несприятливий правовий ефект для особи, не має прийматися виключно на підставі вихідних даних системи дистанційної біометричної ідентифікації.

(36) З метою виконання своїх завдань відповідно до вимог, встановлених у цьому Регламенті, а також у національних нормах, відповідний орган ринкового нагляду та національний орган із захисту даних мають бути повідомлені про кожне використання системи біометричної ідентифікації в режимі реального часу. Органи ринкового нагляду та органи із захисту даних, яким було надіслано повідомлення, мають подавати Комісії щорічний звіт про використання систем біометричної ідентифікації в режимі реального часу.

(37) Крім того, доцільно передбачити у вичерпних рамках, встановлених цим Регламентом, що таке використання на території держави-члена відповідно до цього Регламенту має бути можливим лише там і тою мірою, якою відповідна держава-член вирішила прямо передбачити можливість авторизації такого використання у своїх детальних нормах національного права. Відповідно, держави-члени зберігають свободу відповідно до цього Регламенту взагалі не передбачати таку можливість або передбачати її лише щодо деяких цілей, здатних виправдати авторизоване використання, визначених у цьому Регламенті. Такі національні норми мають бути повідомлені Комісії протягом 30 днів з моменту їх прийняття.

(38) Використання систем ШІ для дистанційної біометричної ідентифікації фізичних осіб у режимі реального часу в загальнодоступних просторах у цілях правоохоронної діяльності неминуче передбачає обробку біометричних даних. Норми цього Регламенту, що забороняють, з урахуванням певних винятків, таке використання і які ґрунтуються на статті 16

ДФЄС, мають застосовуватися як lex specialis щодо норм про обробку біометричних даних, що містяться у статті 10 Директиви (ЄС) 2016/680, таким чином вичерпно регулюючи таке використання та обробку відповідних біометричних даних. Тому таке використання та обробка мають бути можливими лише тою мірою, якою це сумісне з рамками, встановленими цим Регламентом, без того, щоб поза такими рамками компетентні органи, які діють у цілях правоохоронної діяльності, мали можливість використовувати такі системи та обробляти такі дані у зв'язку з цим на підставах, перелічених у статті 10 Директиви (ЄС) 2016/680. У цьому контексті цей Регламент не має на меті забезпечити правову основу для обробки персональних даних відповідно до статті 8 Директиви (ЄС) 2016/680. Однак використання систем дистанційної біометричної ідентифікації в режимі реального часу в загальнодоступних просторах у цілях, відмінних від правоохоронної діяльності, у тому числі компетентними органами, не має охоплюватися конкретними рамками щодо такого використання у цілях правоохоронної діяльності, встановленими цим Регламентом. Таке використання у цілях, відмінних від правоохоронної діяльності, не має тому підпадати під вимогу авторизації відповідно до цього Регламенту та застосовних детальних норм національного права, що можуть надавати чинності такій авторизації.

(39) Будь-яка обробка біометричних даних та інших персональних даних, пов'язана з використанням систем ШІ для біометричної ідентифікації, окрім як у зв'язку з використанням систем дистанційної біометричної ідентифікації в режимі реального часу в загальнодоступних просторах у цілях правоохоронної діяльності, що регулюється цим Регламентом, має продовжувати відповідати всім вимогам, що випливають із статті 10 Директиви (ЄС) 2016/680. Для цілей, відмінних від правоохоронної діяльності, стаття 9(1) Регламенту (ЄС) 2016/679 та стаття 10(1) Регламенту (ЄС) 2018/1725 забороняють обробку біометричних даних з урахуванням обмежених винятків, передбачених у цих статтях. У застосуванні статті 9(1) Регламенту (ЄС) 2016/679

використання дистанційної біометричної ідентифікації у цілях, відмінних від правоохоронної діяльності, вже ставало предметом рішень про заборону з боку національних органів із захисту даних.

(40) Відповідно до статті 6a Протоколу № 21 про позицію Сполученого Королівства та Ірландії щодо простору свободи, безпеки та правосуддя, доданого до ДЄС та ДФЄС, Ірландія не є зобов'язаною нормами, викладеними у статті 5(1), першому підпараграфі, пункті (g), тою мірою, якою він застосовується до використання систем біометричної категоризації для діяльності у сфері поліційного співробітництва та судового співробітництва у кримінальних справах, статті 5(1), першому підпараграфі, пункті (d), тою мірою, якою він застосовується до використання систем ШІ, охоплених цим положенням, статті 5(1), першому підпараграфі, пункті (h), статті 5(2)–(6) та статті 26(10) цього Регламенту, прийнятого на основі статті 16 ДФЄС, які стосуються обробки персональних даних державами-членами під час провадження діяльності, що підпадає під сферу дії розділу 4 або розділу 5 розділу V частини третьої ДФЄС, де Ірландія не є зобов'язаною нормами, що регулюють форми судового співробітництва у кримінальних справах або поліційного співробітництва, які вимагають дотримання положень, викладених на основі статті 16 ДФЄС.

(41) Відповідно до статей 2 і 2a Протоколу № 22 про позицію Данії, доданого до ДЄС та ДФЄС, Данія не є зобов'язаною нормами, викладеними у статті 5(1), першому підпараграфі, пункті (g), тою мірою, якою він застосовується до використання систем біометричної категоризації для діяльності у сфері поліційного співробітництва та судового співробітництва у кримінальних справах, статті 5(1), першому підпараграфі, пункті (d), тою мірою, якою він застосовується до використання систем ШІ, охоплених цим положенням, статті 5(1), першому підпараграфі, пункті (h), (2)–(6) та статті 26(10) цього Регламенту, прийнятого на основі статті 16 ДФЄС, або не підпадає під їх застосування, які стосуються обробки персональних даних державами-членами під час

провадження діяльності, що підпадає під сферу дії розділу 4 або розділу 5 розділу V частини третьої ДФЄС.

(42) Відповідно до презумпції невинуватості, фізичні особи в Союзі мають завжди оцінюватися за їхньою фактичною поведінкою. Фізичні особи не мають ніколи оцінюватися за поведінкою, передбаченою ШІ, виключно на основі їхнього профілювання, рис особистості або характеристик, як-от громадянство, місце народження, місце проживання, кількість дітей, рівень заборгованості або тип автомобіля, без обґрунтованої підозри у причетності такої особи до кримінальної діяльності на основі об'єктивних і перевірюваних фактів та без людської оцінки таких фактів. Тому оцінки ризиків, що здійснюються щодо фізичних осіб з метою оцінки ймовірності вчинення ними правопорушень або прогнозування вчинення фактичного або потенційного кримінального правопорушення виключно на основі їхнього профілювання або оцінки їхніх рис особистості та характеристик, мають бути заборонені. У будь-якому разі ця заборона не стосується і не зачіпає аналітики ризиків, що не ґрунтується на профілюванні осіб або на рисах особистості та характеристиках осіб, — наприклад, систем ШІ, які використовують аналітику ризиків для оцінки ймовірності фінансового шахрайства з боку підприємств на основі підозрілих транзакцій або інструментів аналітики ризиків для прогнозування ймовірності виявлення наркотиків або незаконних товарів митними органами, наприклад на основі відомих маршрутів контрабанди.

(43) Введення в обіг, введення в експлуатацію для цієї конкретної мети або використання систем ШІ, що створюють або розширюють бази даних розпізнавання осіб шляхом нецільового збирання зображень облич з інтернету або записів з камер відеоспостереження, мають бути заборонені, оскільки така практика посилює відчуття масового стеження та може призводити до грубих порушень основоположних прав, у тому числі права на недоторканність приватного життя.

(44) Існують серйозні занепокоєння щодо наукової бази систем ШІ, що прагнуть ідентифікувати або виводити емоції, зокрема у зв'язку з тим, що вираження емоцій суттєво варіюється залежно від культур і ситуацій та навіть у межах однієї особи. До ключових недоліків таких систем належать обмежена надійність, відсутність специфічності та обмежена узагальнюваність. Тому системи ШІ, що ідентифікують або виводять емоції або наміри фізичних осіб на основі їхніх біометричних даних, можуть призводити до дискримінаційних результатів і бути інтрузивними щодо прав і свобод відповідних осіб. З огляду на нерівність сил у контексті праці або освіти в поєднанні з інтрузивним характером цих систем, такі системи можуть призводити до шкідливого або несприятливого поводження з певними фізичними особами або цілими їхніми групами. Тому введення в обіг, введення в експлуатацію або використання систем ШІ, призначених для виявлення емоційного стану осіб у ситуаціях, пов'язаних із робочим місцем та освітою, мають бути заборонені. Ця заборона не має охоплювати системи ШІ, введені в обіг виключно з медичних міркувань або міркувань безпеки, наприклад системи, призначені для терапевтичного використання.

(45) Практики, заборонені правом Союзу, у тому числі законодавством про захист даних, законодавством про недискримінацію, законодавством про захист прав споживачів та конкурентним законодавством, не мають зазнавати впливу з боку цього Регламенту.

(46) Системи ШІ з високим ризиком мають вводитися в обіг на ринку Союзу, вводитися в експлуатацію або використовуватися лише за умови дотримання певних обов'язкових вимог. Ці вимоги мають забезпечити, що системи ШІ з високим ризиком, доступні в Союзі або чиї вихідні дані в інший спосіб використовуються в Союзі, не становлять неприйнятних ризиків для важливих суспільних інтересів Союзу, визнаних та захищених правом Союзу. На основі Нової законодавчої бази, уточненої у повідомленні Комісії «Блакитний посібник із впровадження правил ЄС щодо продуктів 2022 року» (20),

загальне правило полягає в тому, що більш ніж один правовий акт законодавства Союзу про гармонізацію, як-от Регламенти (ЄС) 2017/745 (21) та (ЄС) 2017/746 (22) Європейського Парламенту і Ради або Директива Європейського Парламенту і Ради 2006/42/ЄС (23), може застосовуватися до одного продукту, оскільки надання в користування або введення в експлуатацію може відбуватися лише тоді, коли продукт відповідає всьому застосовному законодавству Союзу про гармонізацію. Для забезпечення узгодженості та уникнення непотрібного адміністративного тягаря або витрат провайдери продукту, що містить одну або більше систем ШІ з високим ризиком, до яких застосовуються вимоги цього Регламенту та законодавства Союзу про гармонізацію, переліченого у додатку до цього Регламенту, мають мати гнучкість щодо операційних рішень про те, як оптимальним чином забезпечити відповідність продукту, що містить одну або більше систем ШІ, усім застосовним вимогам законодавства Союзу про гармонізацію. Системи ШІ, ідентифіковані як такі, що мають високий ризик, мають обмежуватися тими, що мають значний шкідливий вплив на здоров'я, безпеку та основоположні права осіб у Союзі, і таке обмеження має зводити до мінімуму будь-яке можливе обмеження для міжнародної торгівлі.

(47) Системи ШІ можуть мати несприятливий вплив на здоров'я та безпеку осіб, зокрема коли такі системи функціонують як компоненти безпеки продуктів. Відповідно до цілей законодавства Союзу про гармонізацію щодо сприяння вільному пересуванню товарів на внутрішньому ринку та забезпечення того, щоб на ринок потрапляли лише безпечні та в іншому відношенні відповідні продукти, важливо, щоб ризики для безпеки, які можуть генерувати продукти в цілому через їхні цифрові компоненти, у тому числі системи ШІ, належним чином запобігалися та пом'якшувалися. Наприклад, дедалі більш автономні роботи, незалежно від того, чи застосовуються вони у контексті виробництва або особистої допомоги та догляду, мають бути здатні безпечно функціонувати та виконувати свої функції у складних середовищах. Аналогічно, у

секторі охорони здоров'я, де ставки для життя та здоров'я є особливо високими, дедалі більш складні діагностичні системи та системи підтримки людських рішень мають бути надійними та точними.

(48) Ступінь несприятливого впливу, спричиненого системою ШІ, на основоположні права, захищені Хартією, є особливо актуальним при класифікації системи ШІ як такої, що має високий ризик. Ці права включають право на людську гідність, повагу до приватного та сімейного життя, захист персональних даних, свободу вираження поглядів та інформації, свободу зібрань та об'єднань, право на недискримінацію, право на освіту, захист прав споживачів, права працівників, права осіб з інвалідністю, гендерну рівність, права інтелектуальної власності, право на ефективний засіб правового захисту та на справедливий судовий розгляд, право на захист та презумпцію невинуватості, а також право на належне адміністрування. Окрім цих прав, важливо підкреслити, що діти мають особливі права, закріплені в статті 24 Хартії та в Конвенції Організації Об'єднаних Націй про права дитини, додатково розвинуті в Загальному коментарі КПД ООН № 25 щодо цифрового середовища, обидва з яких вимагають урахування вразливостей дітей та надання такого захисту і піклування, як необхідно для їхнього добробуту. Основоположне право на високий рівень захисту довкілля, закріплене в Хартії та реалізоване в політиках Союзу, також має братися до уваги при оцінці тяжкості шкоди, яку може спричинити система ШІ, у тому числі стосовно здоров'я та безпеки осіб.

(49) Щодо систем ШІ з високим ризиком, які є компонентами безпеки продуктів або систем, або які самі є продуктами або системами, що підпадають під сферу дії Регламенту Європейського Парламенту і Ради (ЄС) № 300/2008 (24), Регламенту Європейського Парламенту і Ради (ЄС) № 167/2013 (25), Регламенту Європейського Парламенту і Ради (ЄС) № 168/2013 (26), Директиви Європейського Парламенту і Ради 2014/90/ЄС (27), Директиви Європейського Парламенту і Ради (ЄС)

2016/797 (28), Регламенту Європейського Парламенту і Ради (ЄС) 2018/858 (29), Регламенту Європейського Парламенту і Ради (ЄС) 2018/1139 (30), та Регламенту Європейського Парламенту і Ради (ЄС) 2019/2144 (31), доцільно вносити зміни до цих актів, щоб забезпечити, що Комісія враховує, на основі технічних та регуляторних особливостей кожного сектору та без втручання в існуючі механізми управління, оцінки відповідності та правозастосування і органи, створені в них, обов'язкові вимоги для систем ШІ з високим ризиком, встановлені в цьому Регламенті, під час прийняття будь-яких відповідних делегованих або виконавчих актів на підставі цих актів.

(50) Щодо систем ШІ, які є компонентами безпеки продуктів, або які самі є продуктами, що підпадають під сферу дії певного законодавства Союзу про гармонізацію, переліченого у додатку до цього Регламенту, доцільно класифікувати їх як такі, що мають високий ризик, відповідно до цього Регламенту, якщо відповідний продукт проходить процедуру оцінки відповідності третьою стороною з органом з оцінки відповідності відповідно до цього відповідного законодавства Союзу про гармонізацію. Зокрема, такими продуктами є машини та обладнання, іграшки, ліфти, обладнання та захисні системи, призначені для використання у потенційно вибухонебезпечних атмосферах, радіообладнання, обладнання під тиском, обладнання для водних суден відпочинку, канатні дороги, прилади, що спалюють газоподібне паливо, медичні вироби, in vitro діагностичні медичні вироби, автомобільний та авіаційний транспорт.

(51) Класифікація системи ШІ як такої, що має високий ризик, відповідно до цього Регламенту не має обов'язково означати, що продукт, компонентом безпеки якого є система ШІ, або сама система ШІ як продукт, вважається таким, що має високий ризик, за критеріями, встановленими у відповідному законодавстві Союзу про гармонізацію, що застосовується до продукту. Це стосується, зокрема, Регламентів

(ЄС) 2017/745 та (ЄС) 2017/746, де передбачено оцінку відповідності третьою стороною для продуктів середнього та високого ризику.

(52) Щодо автономних систем ШІ, тобто систем ШІ з високим ризиком, відмінних від тих, що є компонентами безпеки продуктів, або які самі є продуктами, доцільно класифікувати їх як такі, що мають високий ризик, якщо, з огляду на їхню призначену мету, вони становлять високий ризик шкоди для здоров'я та безпеки або основоположних прав осіб, з урахуванням як тяжкості можливої шкоди, так і ймовірності її настання, і вони використовуються у ряді конкретно попередньо визначених областей, зазначених у цьому Регламенті. Ідентифікація цих систем ґрунтується на тій самій методології та критеріях, передбачених також для будь-яких майбутніх змін до переліку систем ШІ з високим ризиком, які Комісія має бути уповноважена приймати за допомогою делегованих актів, з урахуванням швидких темпів технологічного розвитку, а також можливих змін у використанні систем ШІ.

(53) Також важливо уточнити, що можуть бути конкретні випадки, у яких системи ШІ, зазначені у попередньо визначених областях, передбачених у цьому Регламенті, не призводять до значного ризику шкоди для законних інтересів, захищених у цих областях, оскільки вони суттєво не впливають на прийняття рішень або не завдають суттєвої шкоди цим інтересам. Для цілей цього Регламенту система ШІ, яка суттєво не впливає на результат прийняття рішень, має розумітися як система ШІ, що не має впливу на суть і тим самим на результат прийняття рішень, будь то людського чи автоматизованого. Система ШІ, яка суттєво не впливає на результат прийняття рішень, може включати ситуації, у яких виконується одна або більше з наступних умов. Перша така умова має полягати в тому, що система ШІ призначена для виконання вузького процедурного завдання, наприклад системи ШІ, яка перетворює неструктуровані дані на структуровані, системи ШІ, яка класифікує вхідні документи за категоріями, або системи ШІ, яка використовується для виявлення дублікатів серед

великої кількості заявок. Ці завдання є настільки вузькими і обмеженими за своїм характером, що становлять лише обмежені ризики, які не збільшуються внаслідок використання системи ШІ у контексті, зазначеному як такий, що має високий ризик використання, у додатку до цього Регламенту. Друга умова має полягати в тому, що завдання, яке виконує система ШІ, призначене для покращення результату раніше завершеної людської діяльності, яка може бути актуальною для цілей використання з високим ризиком, переліченого у додатку до цього Регламенту. З огляду на ці характеристики система ШІ забезпечує лише додатковий рівень до людської діяльності з відповідно зниженим ризиком. Ця умова застосовувалася б, наприклад, до систем ШІ, призначених для покращення мови, яка використовується у раніше підготовлених документах, наприклад стосовно професійного тону, академічного стилю мови або шляхом узгодження тексту з певним брендовим повідомленням. Третя умова має полягати в тому, що система ШІ призначена для виявлення патернів прийняття рішень або відхилень від попередніх патернів прийняття рішень. Ризик знижуватиметься, оскільки використання системи ШІ слідує за раніше завершеною людською оцінкою, яку вона не покликана замінювати або на яку впливати, без належного людського перегляду. Такі системи ШІ включають, наприклад, ті, які за умови певного патерну виставлення оцінок вчителем можна використовувати для перевірки ex post того, чи міг учитель відхилитися від патерну виставлення оцінок, з метою позначення потенційних невідповідностей або аномалій. Четверта умова має полягати в тому, що система ШІ призначена для виконання завдання, яке є лише підготовчим до оцінки, актуальної для цілей систем ШІ, перелічених у додатку до цього Регламенту, таким чином роблячи можливий вплив вихідних даних системи дуже низьким з точки зору представлення ризику для наступної оцінки. Ця умова охоплює, між іншим, інтелектуальні рішення для роботи з файлами, які включають різні функції від індексації, пошуку, обробки тексту та мовлення або зв'язування даних з іншими джерелами даних, або системи ШІ, що

використовуються для перекладу вихідних документів. У будь-якому разі системи ШІ, що використовуються у варіантах використання з високим ризиком, перелічених у додатку до цього Регламенту, мають вважатися такими, що становлять значні ризики шкоди для здоров'я, безпеки або основоположних прав, якщо система ШІ передбачає профілювання у значенні статті 4, пункт (4) Регламенту (ЄС) 2016/679 або статті 3, пункт (4) Директиви (ЄС) 2016/680 або статті 3, пункт (5) Регламенту (ЄС) 2018/1725. Для забезпечення відстежуваності та прозорості провайдер, який вважає, що система ШІ не є такою, що має високий ризик, на основі умов, зазначених вище, має складати документацію оцінки до введення цієї системи в обіг або в експлуатацію та має надавати цю документацію національним компетентним органам на запит. Такий провайдер має бути зобов'язаний зареєструвати систему ШІ в базі даних ЄС, створеній відповідно до цього Регламенту. З метою надання додаткових вказівок щодо практичного виконання умов, за яких системи ШІ, перелічені у додатку до цього Регламенту, як виняток, не мають високого ризику, Комісія має, після консультацій з Радою з питань ШІ, надати керівні принципи, що визначають таке практичне виконання, доповнені вичерпним переліком практичних прикладів варіантів використання систем ШІ, що мають і не мають високого ризику.

(54) Оскільки біометричні дані становлять особливу категорію персональних даних, доцільно класифікувати як такі, що мають високий ризик, кілька критичних варіантів використання біометричних систем, тією мірою, якою їхнє використання дозволено відповідним правом Союзу та національним правом. Технічні неточності систем ШІ, призначених для дистанційної біометричної ідентифікації фізичних осіб, можуть призводити до упереджених результатів і тягнути за собою дискримінаційні наслідки. Ризик таких упереджених результатів та дискримінаційних наслідків є особливо актуальним щодо віку, етнічного походження, раси, статі або інвалідності. Системи дистанційної біометричної

ідентифікації мають тому класифікуватися як такі, що мають високий ризик, з огляду на ризики, які вони становлять. Така класифікація виключає системи ШІ, призначені для використання в цілях біометричної верифікації, у тому числі автентифікації, єдиною метою яких є підтвердження того, що конкретна фізична особа є тією, за кого вона себе видає, та підтвердження особи фізичної особи з єдиною метою отримання доступу до послуги, розблокування пристрою або безпечного доступу до приміщень. Крім того, системи ШІ, призначені для використання в цілях біометричної категоризації відповідно до чутливих атрибутів або характеристик, захищених статтею 9(1) Регламенту (ЄС) 2016/679, на основі біометричних даних, тією мірою, якою вони не заборонені цим Регламентом, та системи розпізнавання емоцій, не заборонені цим Регламентом, мають класифікуватися як такі, що мають високий ризик. Біометричні системи, що призначені для використання виключно з метою забезпечення заходів кібербезпеки та захисту персональних даних, не мають вважатися системами ШІ з високим ризиком.

(55) Щодо управління та експлуатації критичної інфраструктури доцільно класифікувати як такі, що мають високий ризик, системи ШІ, призначені для використання як компоненти безпеки в управлінні та експлуатації критичної цифрової інфраструктури, переліченої в пункті (8) Додатка до Директиви (ЄС) 2022/2557, дорожнього руху та постачання води, газу, тепла та електроенергії, оскільки їхній вихід з ладу або несправність може наражати на ризик життя та здоров'я осіб у великих масштабах і призводити до помітних порушень у звичайному веденні соціальної та економічної діяльності. Компоненти безпеки критичної інфраструктури, у тому числі критичної цифрової інфраструктури, — це системи, що використовуються для безпосереднього захисту фізичної цілісності критичної інфраструктури або здоров'я та безпеки осіб і майна, але які не є необхідними для функціонування системи. Вихід з ладу або несправність таких компонентів може безпосередньо призводити до ризиків для

фізичної цілісності критичної інфраструктури і тим самим до ризиків для здоров'я та безпеки осіб і майна. Компоненти, призначені для використання виключно у цілях кібербезпеки, не мають кваліфікуватися як компоненти безпеки. Прикладами компонентів безпеки такої критичної інфраструктури можуть бути системи моніторингу тиску води або системи управління пожежною сигналізацією в центрах хмарних обчислень.

(56) Впровадження систем ШІ в освіті важливе для сприяння якісній цифровій освіті та підготовці і надання всім тим, хто навчається, та вчителям можливості набувати та поширювати необхідні цифрові навички та компетенції, у тому числі медіаграмотність та критичне мислення, для активної участі в економіці, суспільстві та демократичних процесах. Однак системи ШІ, що використовуються в освіті або професійній підготовці, зокрема для визначення доступу або прийому, для направлення осіб до навчальних закладів або установ та програм професійної підготовки на всіх рівнях, для оцінки результатів навчання осіб, для оцінки відповідного рівня освіти для особи та суттєвого впливу на рівень освіти та підготовки, який особи отримуватимуть або матимуть можливість отримати, або для моніторингу та виявлення забороненої поведінки студентів під час іспитів, мають класифікуватися як системи ШІ з високим ризиком, оскільки вони можуть визначати освітній та професійний шлях у житті особи і тому можуть впливати на здатність тієї особи забезпечити собі засоби до існування. У разі неналежного проектування та використання такі системи можуть бути особливо інтрузивними та порушувати право на освіту та підготовку, а також право на недискримінацію та увічнювати усталені патерни дискримінації, наприклад, щодо жінок, певних вікових груп, осіб з інвалідністю або осіб певного расового чи етнічного походження або сексуальної орієнтації.

(57) Системи ШІ, що використовуються у сфері зайнятості, управління працівниками та доступу до самозайнятості, зокрема для відбору та підбору персоналу, для прийняття рішень, що впливають на умови трудових відносин,

просування по службі та припинення трудових договірних відносин, для розподілу завдань на основі індивідуальної поведінки, особистісних рис або характеристик та для моніторингу або оцінки осіб у трудових договірних відносинах, також мають класифікуватися як такі, що мають високий ризик, оскільки ці системи можуть мати відчутний вплив на майбутні кар'єрні перспективи, засоби до існування цих осіб та права працівників. Відповідні трудові договірні відносини мають у значущий спосіб охоплювати працівників та осіб, що надають послуги через платформи, як зазначено у Робочій програмі Комісії на 2021 рік. Протягом процесу відбору персоналу та при оцінці, просуванні по службі або утриманні осіб у трудових договірних відносинах такі системи можуть увічнювати усталені патерни дискримінації, наприклад щодо жінок, певних вікових груп, осіб з інвалідністю або осіб певного расового чи етнічного походження або сексуальної орієнтації. Системи ШІ, що використовуються для моніторингу діяльності та поведінки таких осіб, можуть також підривати їхні основоположні права на захист даних та недоторканність приватного життя.

(58) Ще однією сферою, у якій використання систем ШІ заслуговує особливої уваги, є доступ до певних основних приватних та публічних послуг і пільг, необхідних людям для повноцінної участі в суспільстві або для підвищення свого рівня життя, та користування ними. Зокрема, фізичні особи, що подають заяви або отримують основні соціальні допомоги та послуги від публічних органів, а саме послуги охорони здоров'я, виплати у системі соціального забезпечення, соціальні послуги, що забезпечують захист у випадках, як-от материнство, хвороба, виробничі травми, залежність або старість і втрата зайнятості, та соціальну та житлову допомогу, зазвичай залежать від цих допомог та послуг і знаходяться у вразливому становищі стосовно відповідальних органів. Якщо системи ШІ використовуються для визначення того, чи мають такі допомоги та послуги надаватися, відмовлятися у них, зменшуватися, відкликатися або стягуватися органами, у тому числі чи мають бенефіціари законне право на такі допомоги або

послуги, ці системи можуть мати значний вплив на засоби до існування осіб та можуть порушувати їхні основоположні права, наприклад право на соціальний захист, недискримінацію, людську гідність або ефективний засіб правового захисту, і мають тому класифікуватися як такі, що мають високий ризик. Тим не менш, цей Регламент не має перешкоджати розробці та використанню інноваційних підходів у державному управлінні, яке виграло б від ширшого використання відповідних та безпечних систем ШІ, за умови, що ці системи не тягнуть за собою високого ризику для юридичних та фізичних осіб. Крім того, системи ШІ, що використовуються для оцінки кредитного рейтингу або кредитоспроможності фізичних осіб, мають класифікуватися як системи ШІ з високим ризиком, оскільки вони визначають доступ цих осіб до фінансових ресурсів або основних послуг, як-от житло, електроенергія та телекомунікаційні послуги. Системи ШІ, що використовуються для таких цілей, можуть призводити до дискримінації між особами або групами та можуть увічнювати усталені патерни дискримінації, як-то заснованої на расовому чи етнічному походженні, статі, інвалідності, віці або сексуальній орієнтації, або можуть створювати нові форми дискримінаційних впливів. Однак системи ШІ, передбачені правом Союзу з метою виявлення шахрайства у наданні фінансових послуг та у пруденційних цілях для розрахунку вимог до капіталу кредитних установ та страхових компаній, не мають вважатися такими, що мають високий ризик, відповідно до цього Регламенту. Крім того, системи ШІ, призначені для оцінки ризику та ціноутворення стосовно фізичних осіб для медичного та страхування життя, також можуть мати значний вплив на засоби до існування осіб і, якщо їх не розроблено та не використовується належним чином, можуть порушувати їхні основоположні права та призводити до серйозних наслідків для людського життя та здоров'я, у тому числі фінансового відчуження та дискримінації. Нарешті, системи ШІ, що використовуються для оцінки та класифікації екстрених дзвінків від фізичних осіб або для диспетчеризації або

встановлення пріоритетності при диспетчеризації служб першого реагування при надзвичайних ситуаціях, у тому числі поліцією, пожежниками та медичною допомогою, а також систем тріажу пацієнтів у разі надзвичайних ситуацій в охороні здоров'я, мають також класифікуватися як такі, що мають високий ризик, оскільки вони приймають рішення у дуже критичних ситуаціях для життя та здоров'я осіб та їхнього майна.

(59) З огляду на їхню роль та відповідальність, дії правоохоронних органів, що передбачають певне використання систем ШІ, характеризуються значним ступенем нерівності сил і можуть призводити до стеження, арешту або позбавлення свободи фізичної особи, а також інших несприятливих наслідків для основоположних прав, гарантованих Хартією. Зокрема, якщо система ШІ не навчена на якісних даних, не відповідає належним вимогам щодо її продуктивності, точності або стійкості, або не розроблена та протестована належним чином до введення в обіг або іншого введення в експлуатацію, вона може виокремлювати людей дискримінаційним або іншим чином неправильним або несправедливим чином. Крім того, здійснення важливих процедурних основоположних прав, таких як право на ефективний засіб правового захисту та на справедливий судовий розгляд, а також право на захист та презумпцію невинуватості, може бути ускладнено, зокрема, там, де такі системи ШІ не є достатньо прозорими, зрозумілими та задокументованими. Тому доцільно класифікувати як такі, що мають високий ризик, тою мірою, якою їхнє використання дозволено відповідним правом Союзу та національним правом, ряд систем ШІ, призначених для використання у контексті правоохоронної діяльності, де точність, надійність та прозорість є особливо важливими для уникнення несприятливих наслідків, збереження суспільної довіри та забезпечення підзвітності та ефективного відшкодування. З огляду на характер діяльності та пов'язані з нею ризики, ці системи ШІ з високим ризиком мають включати, зокрема, системи ШІ, призначені для

використання правоохоронними органами або від їхнього імені, або установами, органами, відомствами чи агентствами Союзу на підтримку правоохоронних органів для оцінки ризику стати жертвою кримінальних правопорушень для фізичної особи, як-от поліграфи та аналогічні інструменти, для оцінки достовірності доказів у ході розслідування або переслідування кримінальних правопорушень, і, тою мірою, якою це не заборонено цим Регламентом, для оцінки ризику вчинення або повторного вчинення правопорушення фізичною особою не виключно на основі профілювання фізичних осіб або оцінки рис особистості та характеристик або минулої злочинної поведінки фізичних осіб або груп, для профілювання у ході виявлення, розслідування або переслідування кримінальних правопорушень. Системи ШІ, спеціально призначені для використання в адміністративних провадженнях податковими та митними органами, а також підрозділами фінансової розвідки, що виконують адміністративні завдання з аналізу інформації відповідно до законодавства Союзу про протидію відмиванню коштів, не мають класифікуватися як системи ШІ з високим ризиком, що використовуються правоохоронними органами з метою запобігання, виявлення, розслідування та переслідування кримінальних правопорушень. Використання інструментів ШІ правоохоронними та іншими відповідними органами не має ставати чинником нерівності або відчуження. Вплив використання інструментів ШІ на права на захист підозрюваних не має ігноруватися, зокрема складність отримання значущої інформації про функціонування цих систем та відповідна складність оскарження їхніх результатів у суді, зокрема фізичними особами, що перебувають під слідством.

(60) Системи ШІ, що використовуються в управлінні міграцією, притулком та прикордонним контролем, зачіпають осіб, які нерідко перебувають у особливо вразливому становищі та залежать від результатів дій компетентних публічних органів. Точність, недискримінаційний характер та прозорість систем ШІ, що використовуються у цих

контекстах, є тому особливо важливими для гарантування поваги до основоположних прав постраждалих осіб, зокрема їхніх прав на свободу пересування, недискримінацію, захист приватного життя та персональних даних, міжнародний захист та належне адміністрування. Тому доцільно класифікувати як такі, що мають високий ризик, тою мірою, якою їхнє використання дозволено відповідним правом Союзу та національним правом, системи ШІ, призначені для використання компетентними публічними органами або від їхнього імені, або установами, органами, відомствами або агентствами Союзу, яким доручено завдання у сферах управління міграцією, притулком та прикордонним контролем, як-то поліграфи та аналогічні інструменти, для оцінки певних ризиків, що становлять фізичні особи, які в'їжджають на територію держави-члена або подають заяву на отримання візи або притулку, для надання допомоги компетентним публічним органам у вивченні, у тому числі пов'язаній оцінці достовірності доказів, заявок на отримання притулку, візи та дозволів на проживання та пов'язаних скарг стосовно мети встановлення права на отримання статусу для фізичних осіб, що подають заявку, з метою виявлення, розпізнавання або ідентифікації фізичних осіб у контексті управління міграцією, притулком та прикордонним контролем, за винятком перевірки проїзних документів. Системи ШІ у сфері управління міграцією, притулком та прикордонним контролем, охоплені цим Регламентом, мають відповідати відповідним процедурним вимогам, встановленим Регламентом Європейського Парламенту і Ради (ЄС) № 810/2009 (32), Директивою Європейського Парламенту і Ради 2013/32/ЄС (33), та інших відповідних правових актів Союзу. Використання систем ШІ в управлінні міграцією, притулком та прикордонним контролем не має в жодному разі використовуватися державами-членами або установами, органами, відомствами чи агентствами Союзу як засіб уникнення їхніх міжнародних зобов'язань відповідно до Конвенції ООН про статус біженців, укладеної в Женеві 28 липня 1951 року з поправками, внесеними

Протоколом від 31 січня 1967 року. Вони також не мають використовуватися в будь-який спосіб для порушення принципу невислання, або для відмови в безпечних та ефективних законних шляхах на територію Союзу, у тому числі права на міжнародний захист.

(61) Певні системи ШІ, призначені для відправлення правосуддя та демократичних процесів, мають класифікуватися як такі, що мають високий ризик, враховуючи їхній потенційно значний вплив на демократію, верховенство права, індивідуальні свободи, а також право на ефективний засіб правового захисту та справедливий судовий розгляд. Зокрема, для усунення ризиків потенційних упереджень, помилок та непрозорості доцільно кваліфікувати як такі, що мають високий ризик, системи ШІ, призначені для використання судовим органом або від його імені для надання допомоги судовим органам у дослідженні та тлумаченні фактів і права та у застосуванні права до конкретного набору фактів. Системи ШІ, призначені для використання органами альтернативного вирішення спорів для таких цілей, також мають вважатися такими, що мають високий ризик, коли результати провадження з альтернативного вирішення спорів породжують правові наслідки для сторін. Використання інструментів ШІ може підтримувати повноваження суддів щодо прийняття рішень або суддівську незалежність, але не має їх замінювати: остаточне прийняття рішень має залишатися діяльністю, що здійснюється людиною. Класифікація систем ШІ як таких, що мають високий ризик, не має, однак, поширюватися на системи ШІ, призначені для суто допоміжної адміністративної діяльності, що не впливає на фактичне відправлення правосуддя в окремих справах, як-от анонімізація або псевдонімізація судових рішень, документів або даних, комунікація між персоналом, адміністративні завдання.

(62) Без шкоди для норм, передбачених Регламентом Європейського Парламенту і Ради (ЄС) 2024/900 (34), та з метою усунення ризиків неналежного зовнішнього втручання у право голосу, закріплене у статті 39 Хартії, та

несприятливих наслідків для демократії та верховенства права, системи ШІ, призначені для використання з метою впливу на результат виборів або референдуму чи на поведінку фізичних осіб під час голосування на виборах або референдумах, мають класифікуватися як системи ШІ з високим ризиком, за винятком систем ШІ, вихідним даним яких фізичні особи не піддаються безпосередньо, як-от інструменти, що використовуються для організації, оптимізації та структурування політичних кампаній з адміністративної та логістичної точки зору.

(63) Той факт, що система ШІ класифікується як система ШІ з високим ризиком відповідно до цього Регламенту, не має тлумачитися як вказівка на те, що використання системи є законним відповідно до інших актів права Союзу або відповідно до національного права, сумісного з правом Союзу, наприклад щодо захисту персональних даних, використання поліграфів та аналогічних інструментів або інших систем для виявлення емоційного стану фізичних осіб. Будь-яке таке використання має продовжуватися виключно відповідно до застосовних вимог, що випливають із Хартії та застосовних актів вторинного права Союзу та національного права. Цей Регламент не має розумітися як такий, що передбачає правову підставу для обробки персональних даних, у тому числі особливих категорій персональних даних, де це доречно, якщо цим Регламентом спеціально не передбачено інше.

(64) Для пом'якшення ризиків від систем ШІ з високим ризиком, введених в обіг або в експлуатацію, та забезпечення високого рівня довіреності до певних систем ШІ з високим ризиком мають застосовуватися певні обов'язкові вимоги з урахуванням призначеної мети та контексту використання системи ШІ та відповідно до системи управління ризиками, що має бути створена провайдером. Заходи, прийняті провайдерами для дотримання обов'язкових вимог цього Регламенту, мають враховувати загальновизнаний сучасний стан розвитку ШІ, бути пропорційними та ефективними для досягнення цілей цього

Регламенту. На основі Нової законодавчої бази, уточненої у повідомленні Комісії «Блакитний посібник із впровадження правил ЄС щодо продуктів 2022 року», загальне правило полягає в тому, що більш ніж один правовий акт законодавства Союзу про гармонізацію може застосовуватися до одного продукту, оскільки надання в користування або введення в експлуатацію може відбуватися лише тоді, коли продукт відповідає всьому застосовному законодавству Союзу про гармонізацію. Небезпеки систем ШІ, охоплені вимогами цього Регламенту, стосуються інших аспектів, ніж існуюче законодавство Союзу про гармонізацію, і тому вимоги цього Регламенту доповнюватимуть існуючий масив законодавства Союзу про гармонізацію. Наприклад, продукти у вигляді машин та обладнання або медичних виробів, що включають систему ШІ, можуть становити ризики, не охоплені основними вимогами до охорони здоров'я та безпеки, встановленими у відповідному гармонізованому законодавстві Союзу, оскільки таке галузеве законодавство не стосується ризиків, специфічних для систем ШІ. Це вимагає одночасного та взаємодоповнювального застосування різних законодавчих актів. Для забезпечення узгодженості та уникнення непотрібного адміністративного тягаря і непотрібних витрат провайдери продукту, що містить одну або більше систем ШІ з високим ризиком, до яких застосовуються вимоги цього Регламенту та законодавства Союзу про гармонізацію, заснованого на Новій законодавчій базі та переліченого у додатку до цього Регламенту, мають мати гнучкість щодо операційних рішень про те, як оптимальним чином забезпечити відповідність продукту, що містить одну або більше систем ШІ, усім застосовним вимогам цього гармонізованого законодавства Союзу. Така гнучкість може означати, наприклад, рішення провайдера інтегрувати частину необхідних процесів тестування та звітності, інформації та документації, що вимагаються цим Регламентом, до вже існуючих документів та процедур, що вимагаються відповідно до існуючого законодавства Союзу про гармонізацію, заснованого на Новій законодавчій

базі та переліченого у додатку до цього Регламенту. Це жодним чином не має підривати зобов'язання провайдера виконувати всі застосовні вимоги.

(65) Система управління ризиками має складатися з безперервного ітеративного процесу, який планується та здійснюється протягом усього життєвого циклу системи ШІ з високим ризиком. Цей процес має бути спрямований на виявлення та пом'якшення відповідних ризиків систем ШІ для здоров'я, безпеки та основоположних прав. Система управління ризиками має регулярно переглядатися та оновлюватися для забезпечення її подальшої ефективності, а також обґрунтування та документування будь-яких значущих рішень і дій, вжитих відповідно до цього Регламенту. Цей процес має забезпечувати, що провайдер виявляє ризики або несприятливі наслідки та вживає заходів щодо їх пом'якшення для відомих та розумно передбачуваних ризиків систем ШІ для здоров'я, безпеки та основоположних прав з огляду на їхню призначену мету та розумно передбачуване неналежне використання, у тому числі можливі ризики, що виникають внаслідок взаємодії між системою ШІ та середовищем, у якому вона функціонує. Система управління ризиками має приймати найбільш відповідні заходи управління ризиками з огляду на сучасний стан розвитку ШІ. При визначенні найбільш відповідних заходів управління ризиками провайдер має документувати та пояснювати зроблені вибори та, де доречно, залучати експертів та зовнішніх зацікавлених сторін. При визначенні розумно передбачуваного неналежного використання систем ШІ з високим ризиком провайдер має охоплювати варіанти використання систем ШІ, які, хоча й не охоплені безпосередньо призначеною метою та передбачені в інструкції з використання, тим не менш можуть розумно очікуватися як результат легко передбачуваної людської поведінки в контексті конкретних характеристик та використання конкретної системи ШІ. Будь-які відомі або передбачувані обставини, пов'язані з використанням системи ШІ з високим ризиком відповідно до її призначеної мети або в умовах розумно

передбачуваного неналежного використання, які можуть призводити до ризиків для здоров'я та безпеки або основоположних прав, мають включатися до інструкцій з використання, що надаються провайдером. Це робиться для того, щоб суб'єкт розгортання був обізнаний про них та враховував їх при використанні системи ШІ з високим ризиком. Виявлення та впровадження заходів щодо пом'якшення ризиків для передбачуваного неналежного використання відповідно до цього Регламенту не має вимагати конкретного додаткового навчання системи ШІ з високим ризиком провайдером для усунення передбачуваного неналежного використання. Проте провайдерам рекомендується розглянути такі додаткові заходи навчання для пом'якшення розумно передбачуваних видів неналежного використання, наскільки це необхідно і доречно.

(66) До систем ШІ з високим ризиком мають застосовуватися вимоги щодо управління ризиками, якості та релевантності використовуваних наборів даних, технічної документації та ведення записів, прозорості та надання інформації суб'єктам розгортання, нагляду з боку людини, а також стійкості, точності та кібербезпеки. Ці вимоги необхідні для ефективного пом'якшення ризиків для здоров'я, безпеки та основоположних прав. Оскільки жодних інших менш обмежувальних для торгівлі заходів розумно не існує, ці вимоги не є невиправданими обмеженнями торгівлі.

(67) Якісні дані та доступ до якісних даних відіграють ключову роль у структуруванні та забезпеченні продуктивності багатьох систем ШІ, особливо коли використовуються методи, що передбачають навчання моделей, з метою забезпечення того, щоб система ШІ з високим ризиком функціонувала за призначенням та безпечно і не ставала джерелом дискримінації, забороненої правом Союзу. Якісні набори даних для навчання, перевірки та тестування вимагають впровадження належних практик управління та менеджменту даних. Набори даних для навчання, перевірки та тестування, включаючи мітки, мають бути релевантними, достатньо репрезентативними та по можливості

вільними від помилок і повними з огляду на призначену мету системи. Для сприяння дотриманню законодавства Союзу про захист даних, наприклад Регламенту (ЄС) 2016/679, практики управління та менеджменту даних мають включати у випадку персональних даних прозорість щодо первісної мети збору даних. Набори даних також мають мати відповідні статистичні властивості, у тому числі стосовно осіб або груп осіб, щодо яких призначена система ШІ з високим ризиком, з особливою увагою до пом'якшення можливих упереджень у наборах даних, які, ймовірно, впливатимуть на здоров'я та безпеку осіб, матимуть негативний вплив на основоположні права або призводитимуть до дискримінації, забороненої правом Союзу, особливо там, де вихідні дані впливають на вхідні дані для майбутніх операцій (петлі зворотного зв'язку). Упередження можуть, наприклад, бути властивими базовим наборам даних, особливо коли використовуються історичні дані, або виникати при впровадженні систем у реальних умовах. Результати, що надаються системами ШІ, можуть зазнавати впливу таких притаманних упереджень, які схильні поступово наростати і тим самим увічнювати та посилювати існуючу дискримінацію, зокрема стосовно осіб, що належать до певних вразливих груп, у тому числі расових або етнічних груп. Вимога про те, щоб набори даних по можливості були повними та вільними від помилок, не має впливати на використання технологій забезпечення конфіденційності в контексті розробки та тестування систем ШІ. Зокрема, набори даних мають враховувати тією мірою, якою це вимагається їхньою призначеною метою, риси, характеристики або елементи, притаманні конкретному географічному, контекстуальному, поведінковому або функціональному середовищу, в якому призначена до використання система ШІ. Вимоги щодо управління даними можуть виконуватися шляхом звернення до третіх сторін, що пропонують сертифіковані послуги дотримання відповідності, включаючи перевірку управління даними, цілісності наборів даних та практик

навчання, перевірки та тестування даних, тією мірою, якою забезпечується відповідність вимогам до даних цього Регламенту.

(68) Для розробки та оцінки систем ШІ з високим ризиком певні суб'єкти, зокрема провайдери, нотифіковані органи та інші відповідні суб'єкти, наприклад Центри цифрових інновацій Європи, випробувальні та дослідницькі установи та дослідники, мають мати можливість доступу та використання якісних наборів даних у сферах діяльності цих суб'єктів, пов'язаних із цим Регламентом. Загальноєвропейські простори даних, створені Комісією, та сприяння обміну даними між підприємствами та з урядом в суспільних інтересах сприятимуть забезпеченню надійного, підзвітного та недискримінаційного доступу до якісних даних для навчання, перевірки та тестування систем ШІ. Наприклад, у сфері охорони здоров'я Європейський простір даних охорони здоров'я сприятиме недискримінаційному доступу до медичних даних та навчанню алгоритмів ШІ на цих наборах даних у спосіб, що зберігає конфіденційність, безпечним, своєчасним, прозорим та надійним чином та з відповідним інституційним управлінням. Відповідні компетентні органи, у тому числі галузеві, що забезпечують або підтримують доступ до даних, також можуть підтримувати надання якісних даних для навчання, перевірки та тестування систем ШІ.

(69) Право на недоторканність приватного життя та захист персональних даних має гарантуватися протягом усього життєвого циклу системи ШІ. У цьому відношенні принципи мінімізації даних та захисту даних за задумом та за замовчуванням, як передбачено законодавством Союзу про захист даних, застосовуються при обробці персональних даних. Заходи, вжиті провайдерами для забезпечення дотримання цих принципів, можуть включати не лише анонімізацію та шифрування, але й використання технологій, що дозволяють доставляти алгоритми до даних та навчати системи ШІ без передачі між сторонами або копіювання самих необроблених або

структурованих даних, без шкоди для вимог щодо управління даними, передбачених у цьому Регламенті.

(70) З метою захисту права інших від дискримінації, яка може виникнути внаслідок упередженості в системах ШІ, провайдери мають, як виняток, тією мірою, якою це суворо необхідно для забезпечення виявлення та виправлення упередженості стосовно систем ШІ з високим ризиком, за умови відповідних гарантій основоположних прав і свобод фізичних осіб і після застосування всіх застосовних умов, встановлених цим Регламентом, на додаток до умов, встановлених Регламентами (ЄС) 2016/679 та (ЄС) 2018/1725 і Директивою (ЄС) 2016/680, мати можливість також обробляти особливі категорії персональних даних як питання суттєвого суспільного інтересу у значенні статті 9(2), пункту (g) Регламенту (ЄС) 2016/679 та статті 10(2), пункту (g) Регламенту (ЄС) 2018/1725.

(71) Наявність зрозумілої інформації про те, як системи ШІ з високим ризиком були розроблені та як вони функціонують протягом усього свого терміну служби, є важливою умовою для забезпечення відстежуваності цих систем, перевірки відповідності вимогам цього Регламенту, а також моніторингу їхньої роботи та моніторингу після введення в обіг. Для цього необхідно вести записи та мати в наявності технічну документацію, що містить інформацію, необхідну для оцінки відповідності системи ШІ відповідним вимогам та сприяння моніторингу після введення в обіг. Така інформація має включати загальні характеристики, можливості та обмеження системи, алгоритми, дані, процеси навчання, тестування та перевірки, що використовуються, а також документацію щодо відповідної системи управління ризиками, складену у зрозумілій та вичерпній формі. Технічна документація має зберігатися в актуальному стані належним чином протягом усього терміну служби системи ШІ. Крім того, системи ШІ з високим ризиком мають технічно

забезпечувати автоматичну реєстрацію подій за допомогою журналів протягом усього терміну служби системи.

(72) Для вирішення проблем, пов'язаних з непрозорістю та складністю певних систем ШІ, та надання суб'єктам розгортання допомоги у виконанні їхніх зобов'язань відповідно до цього Регламенту, для систем ШІ з високим ризиком до їхнього введення в обіг або в експлуатацію має вимагатися прозорість. Системи ШІ з високим ризиком мають проектуватися таким чином, щоб суб'єкти розгортання могли розуміти принцип роботи системи ШІ, оцінювати її функціональність та розуміти її переваги та обмеження. Системи ШІ з високим ризиком мають супроводжуватися відповідною інформацією у формі інструкцій з використання. Така інформація має включати характеристики, можливості та обмеження продуктивності системи ШІ. Вони охоплюватимуть інформацію про можливі відомі та передбачувані обставини, пов'язані з використанням системи ШІ з високим ризиком, у тому числі дії суб'єкта розгортання, що можуть впливати на поведінку та продуктивність системи, за яких система ШІ може призводити до ризиків для здоров'я, безпеки та основоположних прав, про зміни, попередньо визначені та оцінені провайдером щодо відповідності, та про відповідні заходи нагляду з боку людини, у тому числі заходи для сприяння інтерпретації вихідних даних системи ШІ суб'єктами розгортання. Прозорість, у тому числі інструкції з використання, що додаються, має допомагати суб'єктам розгортання у використанні системи та підтримувати прийняття ними обґрунтованих рішень. Суб'єкти розгортання мають, між іншим, бути у кращому становищі для здійснення правильного вибору системи, яку вони мають намір використовувати, з огляду на застосовні до них зобов'язання, бути поінформованими про призначені та виключені варіанти використання та використовувати систему ШІ правильно та в належний спосіб. З метою підвищення читабельності та доступності інформації, що включається до інструкцій з використання, де доречно, мають включатися ілюстративні приклади, наприклад щодо

обмежень та призначених і виключених варіантів використання системи ШІ. Провайдери мають забезпечити, щоб уся документація, у тому числі інструкції з використання, містила змістовну, вичерпну, доступну та зрозумілу інформацію, враховуючи потреби та передбачувані знання цільових суб'єктів розгортання. Інструкції з використання мають надаватися мовою, яка може бути легко зрозуміла цільовим суб'єктам розгортання, як це визначається відповідною державою-членом.

(73) Системи ШІ з високим ризиком мають проектуватися та розроблятися таким чином, щоб фізичні особи могли здійснювати нагляд за їхнім функціонуванням, забезпечувати їхнє використання за призначенням та те, що їхні наслідки враховуються протягом усього життєвого циклу системи. З цією метою провайдер системи має визначити відповідні заходи нагляду з боку людини до введення системи в обіг або в експлуатацію. Зокрема, де доречно, такі заходи мають гарантувати, що система підпорядкована вбудованим операційним обмеженням, які не можуть бути відмінені самою системою, та реагує на людського оператора, а фізичні особи, яким доручено нагляд з боку людини, мають необхідну компетентність, підготовку та повноваження для виконання цієї ролі. Також важливо, де доречно, забезпечити, щоб системи ШІ з високим ризиком включали механізми для керівництва та інформування фізичної особи, якій доручено нагляд з боку людини, для прийняття обґрунтованих рішень про те, чи, коли і як втрутитися з метою уникнення негативних наслідків або ризиків, або для зупинення системи, якщо вона не функціонує за призначенням. Враховуючи значні наслідки для осіб у випадку неправильного зіставлення певними системами біометричної ідентифікації, доцільно передбачити розширену вимогу нагляду з боку людини для таких систем, щоб жодні дії або рішення не могли прийматися суб'єктом розгортання на основі ідентифікації, що є результатом системи, якщо це не було окремо верифіковано та підтверджено щонайменше двома фізичними особами. Ці особи можуть бути

з одного або більше суб'єктів і включати особу, яка управляє системою або використовує її. Ця вимога не має створювати непотрібного тягаря або затримок, і може бути достатнім, щоб окремі верифікації різними особами автоматично реєструвалися в журналах, що генеруються системою. З огляду на специфіку сфер правоохоронної діяльності, міграції, прикордонного контролю та притулку, ця вимога не має застосовуватися там, де право Союзу або національне право вважає застосування цієї вимоги непропорційним.

(74) Системи ШІ з високим ризиком мають стабільно функціонувати протягом усього свого життєвого циклу та відповідати належному рівню точності, стійкості та кібербезпеки з огляду на їхню призначену мету та відповідно до загальновизнаного сучасного стану розвитку технологій. Комісії та відповідним організаціям та зацікавленим сторонам рекомендується приділяти належну увагу пом'якшенню ризиків та негативних наслідків системи ШІ. Очікуваний рівень показників продуктивності має бути задекларований в інструкціях з використання, що додаються. Провайдерам рекомендується доносити цю інформацію до суб'єктів розгортання у зрозумілий та легко доступний спосіб, вільний від непорозумінь або оманливих тверджень. Законодавство Союзу про юридичну метрологію, у тому числі Директиви 2014/31/ЄС (35) та 2014/32/ЄС (36) Європейського Парламенту і Ради спрямоване на забезпечення точності вимірювань та сприяння прозорості та справедливості комерційних операцій. У цьому контексті у співпраці з відповідними зацікавленими сторонами та організаціями, наприклад органами з метрології та порівняльного оцінювання, Комісія має заохочувати, де доречно, розробку еталонів та методологій вимірювання для систем ШІ. При цьому Комісія має приймати до відома та співпрацювати з міжнародними партнерами, що працюють над метрологією та відповідними показниками вимірювання, пов'язаними з ШІ.

(75) Технічна стійкість є ключовою вимогою для систем ШІ з високим ризиком. Вони мають бути стійкими стосовно шкідливої або іншим чином небажаної поведінки, яка може бути наслідком обмежень у самих системах або в середовищі, в якому системи функціонують (наприклад, помилки, несправності, невідповідності, непередбачені ситуації). Тому мають вживатися технічні та організаційні заходи для забезпечення стійкості систем ШІ з високим ризиком, наприклад шляхом проектування та розробки відповідних технічних рішень для запобігання або мінімізації шкідливої або іншим чином небажаної поведінки. Такі технічні рішення можуть включати, наприклад, механізми, що дозволяють системі безпечно переривати свою роботу (плани безпечного відмовлення) за наявності певних аномалій або коли функціонування відбувається за межами певних попередньо встановлених меж. Невдача у захисті від цих ризиків може призводити до наслідків для безпеки або негативно впливати на основоположні права, наприклад внаслідок помилкових рішень або неправильних чи упереджених вихідних даних, генерованих системою ШІ.

(76) Кібербезпека відіграє вирішальну роль у забезпеченні стійкості систем ШІ до спроб змінити їхнє використання, поведінку, продуктивність або скомпрометувати їхні властивості безпеки з боку зловмисних третіх сторін, що використовують уразливості системи. Кібератаки на системи ШІ можуть використовувати специфічні для ШІ активи, наприклад навчальні набори даних (як-от отруєння даних) або навчені моделі (наприклад, атаки на основі змагального прикладу або визначення належності до навчальної вибірки), або використовувати уразливості в цифрових активах системи ШІ або базовій ІКТ-інфраструктурі. Щоб забезпечити рівень кібербезпеки, відповідний ризикам, провайдерами систем ШІ з високим ризиком мають вживатися відповідні заходи, наприклад засоби контролю безпеки, також з урахуванням, де доречно, базової ІКТ-інфраструктури.

(77) Без шкоди для вимог щодо стійкості та точності, встановлених у цьому Регламенті, системи ШІ з високим ризиком, що підпадають під сферу дії Регламенту Європейського Парламенту і Ради про горизонтальні вимоги до кібербезпеки продуктів з цифровими елементами, відповідно до цього регламенту можуть демонструвати дотримання вимог кібербезпеки цього Регламенту шляхом виконання основних вимог кібербезпеки, встановлених у тому регламенті. Якщо системи ШІ з високим ризиком виконують основні вимоги Регламенту Європейського Парламенту і Ради про горизонтальні вимоги до кібербезпеки продуктів з цифровими елементами, вони мають вважатися такими, що відповідають вимогам кібербезпеки, встановленим у цьому Регламенті, тою мірою, якою досягнення цих вимог продемонстровано в ЄС-декларації про відповідність або її частинах, виданих відповідно до того регламенту. З цією метою оцінка ризиків кібербезпеки, пов'язаних із продуктом з цифровими елементами, класифікованим як система ШІ з високим ризиком відповідно до цього Регламенту, що здійснюється відповідно до Регламенту Європейського Парламенту і Ради про горизонтальні вимоги до кібербезпеки продуктів з цифровими елементами, має розглядати ризики для кіберстійкості системи ШІ щодо спроб неавторизованих третіх сторін змінити її використання, поведінку або продуктивність, у тому числі вразливості, специфічні для ШІ, такі як отруєння даних або атаки на основі змагального прикладу, а також, де доречно, ризики для основоположних прав, як того вимагає цей Регламент.

(78) Процедура оцінки відповідності, передбачена цим Регламентом, має застосовуватися стосовно основних вимог кібербезпеки продукту з цифровими елементами, охопленого Регламентом Європейського Парламенту і Ради про горизонтальні вимоги до кібербезпеки продуктів з цифровими елементами та класифікованого як система ШІ з високим ризиком відповідно до цього Регламенту. Однак це правило не має призводити до зниження необхідного рівня забезпечення безпеки

критичних продуктів з цифровими елементами, охоплених Регламентом Європейського Парламенту і Ради про горизонтальні вимоги до кібербезпеки продуктів з цифровими елементами. Тому, шляхом відступу від цього правила, системи ШІ з високим ризиком, що підпадають під сферу дії цього Регламенту та також кваліфіковані як важливі та критичні продукти з цифровими елементами відповідно до Регламенту Європейського Парламенту і Ради про горизонтальні вимоги до кібербезпеки продуктів з цифровими елементами, до яких застосовується процедура оцінки відповідності на основі внутрішнього контролю, встановлена у додатку до цього Регламенту, підпорядковуються положенням про оцінку відповідності Регламенту Європейського Парламенту і Ради про горизонтальні вимоги до кібербезпеки продуктів з цифровими елементами тою мірою, якою це стосується основних вимог кібербезпеки того регламенту. У цьому випадку щодо всіх інших аспектів, охоплених цим Регламентом, мають застосовуватися відповідні положення про оцінку відповідності на основі внутрішнього контролю, встановлені у додатку до цього Регламенту. Спираючись на знання та досвід ENISA в галузі політики кібербезпеки та завдань, покладених на ENISA відповідно до Регламенту Європейського Парламенту і Ради (ЄС) 2019/881 (37), Комісія має співпрацювати з ENISA з питань, пов'язаних із кібербезпекою систем ШІ.

(79) Доцільно, щоб конкретна фізична або юридична особа, визначена як провайдер, брала на себе відповідальність за введення в обіг або введення в експлуатацію системи ШІ з високим ризиком незалежно від того, чи є ця фізична або юридична особа особою, яка спроектувала або розробила систему.

(80) Як підписанти Конвенції Організації Об'єднаних Націй про права осіб з інвалідністю, Союз та держави-члени юридично зобов'язані захищати осіб з інвалідністю від дискримінації та сприяти їхній рівності, забезпечувати, щоб особи з інвалідністю мали доступ на рівних засадах з іншими до інформаційно-комунікаційних технологій та систем, та забезпечувати повагу до

конфіденційності осіб з інвалідністю. З огляду на зростаюче значення та використання систем ШІ застосування принципів універсального дизайну до всіх нових технологій і послуг має забезпечувати повний та рівний доступ для всіх, хто потенційно зазнає впливу ШІ-технологій або їх використовує, у тому числі для осіб з інвалідністю, у спосіб, що повною мірою враховує їхню притаманну гідність та різноманітність. Тому провайдерам важливо забезпечувати повне дотримання вимог доступності, у тому числі Директиви Європейського Парламенту і Ради (ЄС) 2016/2102 (38) та Директиви (ЄС) 2019/882. Провайдери мають забезпечувати дотримання цих вимог за задумом. Тому необхідні заходи мають інтегруватися якомога більше в дизайн системи ШІ з високим ризиком.

(81) Провайдер має створити надійну систему управління якістю, забезпечити виконання необхідної процедури оцінки відповідності, складати відповідну документацію та створити надійну систему моніторингу після введення в обіг. Провайдери систем ШІ з високим ризиком, що підпадають під зобов'язання щодо систем управління якістю відповідно до відповідного галузевого права Союзу, мають мати можливість включати елементи системи управління якістю, передбаченої цим Регламентом, як частину існуючої системи управління якістю, передбаченої тим іншим галузевим правом Союзу. Взаємодоповнюваність між цим Регламентом та існуючим галузевим правом Союзу також має враховуватися в майбутній діяльності зі стандартизації або вказівках, прийнятих Комісією. Публічні органи, що вводять в експлуатацію системи ШІ з високим ризиком для власного використання, можуть приймати та впроваджувати правила для системи управління якістю як частину системи управління якістю, прийнятої на національному або регіональному рівні, де доречно, з урахуванням специфіки сектору та компетенцій і організації відповідного публічного органу.

(82) Для забезпечення виконання цього Регламенту та створення рівних умов для операторів, а також з урахуванням різних форм надання в

користування цифрових продуктів важливо забезпечити, щоб за будь-яких обставин особа, заснована в Союзі, могла надавати органам усю необхідну інформацію про відповідність системи ШІ. Тому до надання своїх систем ШІ в користування в Союзі провайдери, засновані в третіх країнах, мають шляхом письмового доручення призначати уповноваженого представника, заснованого в Союзі. Цей уповноважений представник відіграє ключову роль у забезпеченні відповідності систем ШІ з високим ризиком, введених в обіг або в експлуатацію в Союзі тими провайдерами, які не засновані в Союзі, та у виконанні функції їхньої контактної особи, заснованої в Союзі.

(83) З огляду на природу та складність ланцюга створення вартості для систем ШІ та відповідно до Нової законодавчої бази важливо забезпечити правову визначеність та сприяти дотриманню цього Регламенту. Тому необхідно уточнити роль і конкретні зобов'язання відповідних операторів у цьому ланцюгу створення вартості, наприклад імпортерів та дистриб'юторів, які можуть сприяти розробці систем ШІ. У певних ситуаціях ці оператори можуть одночасно виконувати більше однієї ролі і тому мають сукупно виконувати всі відповідні зобов'язання, пов'язані з цими ролями. Наприклад, оператор може одночасно виступати дистриб'ютором та імпортером.

(84) Для забезпечення правової визначеності необхідно уточнити, що за певних конкретних умов будь-який дистриб'ютор, імпортер, суб'єкт розгортання або інша третя сторона мають вважатися провайдером системи ШІ з високим ризиком і тому брати на себе всі відповідні зобов'язання. Це стосувалося б випадку, якщо ця сторона розміщує своє найменування або торгову марку на системі ШІ з високим ризиком, вже введеній в обіг або в експлуатацію, без шкоди для договірних домовленостей, що передбачають інший розподіл зобов'язань. Це також стосувалося б випадку, якщо ця сторона вносить суттєву модифікацію до системи ШІ з високим ризиком, яка вже була введена в обіг або вже введена в експлуатацію, таким чином, що вона залишається системою ШІ з високим ризиком

відповідно до цього Регламенту, або якщо вона змінює призначену мету системи ШІ, у тому числі системи ШІ загального призначення, що не була класифікована як така, що має високий ризик, та вже була введена в обіг або введена в експлуатацію, таким чином, що система ШІ стає системою ШІ з високим ризиком відповідно до цього Регламенту. Ці положення мають застосовуватися без шкоди для більш конкретних положень, встановлених у певному законодавстві Союзу про гармонізацію, заснованому на Новій законодавчій базі, разом із яким має застосовуватися цей Регламент. Наприклад, стаття 16(2) Регламенту (ЄС) 2017/745, яка встановлює, що певні зміни не мають вважатися модифікаціями пристрою, що можуть впливати на його відповідність застосовним вимогам, має продовжувати застосовуватися до систем ШІ з високим ризиком, які є медичними виробами у значенні того Регламенту.

(85) Системи ШІ загального призначення можуть самі по собі використовуватися як системи ШІ з високим ризиком або бути компонентами інших систем ШІ з високим ризиком. Тому з огляду на їхній особливий характер та для забезпечення справедливого розподілу відповідальності у ланцюгу створення вартості ШІ провайдери таких систем мають, незалежно від того, чи вони можуть використовуватися як системи ШІ з високим ризиком як такі іншими провайдерами або як компоненти систем ШІ з високим ризиком, та якщо цим Регламентом не передбачено інше, тісно співпрацювати з провайдерами відповідних систем ШІ з високим ризиком для забезпечення їхньої відповідності відповідним зобов'язанням відповідно до цього Регламенту та з компетентними органами, створеними відповідно до цього Регламенту.

(86) У випадках, коли відповідно до умов, встановлених у цьому Регламенті, провайдер, який спочатку ввів систему ШІ в обіг або ввів її в експлуатацію, більше не має вважатися провайдером для цілей цього Регламенту, і коли цей провайдер прямо не виключив перетворення системи ШІ на систему ШІ з високим ризиком, колишній провайдер тим не менш має тісно

співпрацювати та надавати необхідну інформацію і забезпечувати розумно очікуваний технічний доступ та іншу допомогу, необхідні для виконання зобов'язань, встановлених у цьому Регламенті, зокрема щодо дотримання оцінки відповідності систем ШІ з високим ризиком.

(87) Крім того, якщо система ШІ з високим ризиком, яка є компонентом безпеки продукту, що підпадає під сферу дії законодавства Союзу про гармонізацію, заснованого на Новій законодавчій базі, не вводиться в обіг або в експлуатацію незалежно від продукту, виробник продукту, визначений у тому законодавстві, має виконувати зобов'язання провайдера, встановлені у цьому Регламенті, та має, зокрема, забезпечувати, що система ШІ, вбудована в кінцевий продукт, відповідає вимогам цього Регламенту.

(88) У ланцюгу створення вартості ШІ численні сторони часто постачають системи ШІ, інструменти та послуги, а також компоненти або процеси, що включаються провайдером до системи ШІ з різними цілями, у тому числі навчання моделі, перенавчання моделі, тестування та оцінка моделі, інтеграція в програмне забезпечення або інші аспекти розробки моделі. Ці сторони відіграють важливу роль у ланцюгу створення вартості стосовно провайдера системи ШІ з високим ризиком, до якої інтегруються їхні системи ШІ, інструменти, послуги, компоненти або процеси, та мають шляхом письмової угоди надавати цьому провайдеру необхідну інформацію, можливості, технічний доступ та іншу допомогу на основі загальновизнаного сучасного стану розвитку технологій, щоб дати провайдеру можливість повністю виконувати зобов'язання, встановлені у цьому Регламенті, не порушуючи власних прав інтелектуальної власності або комерційної таємниці.

(89) Третіх сторін, що забезпечують публічний доступ до інструментів, послуг, процесів або компонентів ШІ, відмінних від моделей ШІ загального призначення, не слід зобов'язувати виконувати вимоги, що стосуються відповідальності у ланцюгу створення вартості ШІ, зокрема стосовно провайдера, який їх

використовував або інтегрував, якщо ці інструменти, послуги, процеси або компоненти ШІ надаються у публічний доступ на умовах вільної ліцензії з відкритим вихідним кодом. Розробників вільних інструментів, послуг, процесів або компонентів ШІ з відкритим вихідним кодом, відмінних від моделей ШІ загального призначення, слід заохочувати до впровадження широко поширених практик документування, таких як картки моделей та технічні паспорти даних, як спосіб прискорення обміну інформацією у ланцюгу створення вартості ШІ, що дозволяє сприяти розвитку надійних систем ШІ в Союзі.

(90) Комісія могла б розробляти та рекомендувати добровільні типові договірні умови між провайдерами систем ШІ з високим ризиком та третіми сторонами, що постачають інструменти, послуги, компоненти або процеси, що використовуються або інтегруються в системи ШІ з високим ризиком, для сприяння співпраці у ланцюгу створення вартості. При розробці добровільних типових договірних умов Комісія також має враховувати можливі договірні вимоги, застосовні в конкретних секторах або бізнес-кейсах.

(91) З огляду на природу систем ШІ та ризики для безпеки та основоположних прав, можливо пов'язані з їхнім використанням, у тому числі щодо необхідності забезпечення належного моніторингу продуктивності системи ШІ в реальних умовах, доцільно встановити конкретні обов'язки для суб'єктів розгортання. Суб'єкти розгортання мають, зокрема, вживати відповідних технічних та організаційних заходів для забезпечення використання ними систем ШІ з високим ризиком відповідно до інструкцій з використання, а певні інші зобов'язання мають бути передбачені стосовно моніторингу функціонування систем ШІ та щодо ведення записів, де доречно. Крім того, суб'єкти розгортання мають забезпечувати, щоб особи, яким доручено реалізацію інструкцій з використання та нагляду з боку людини, як передбачено цим Регламентом, мали необхідну компетентність, зокрема достатній рівень

грамотності у сфері ШІ, підготовку та повноваження для належного виконання цих завдань. Ці зобов'язання мають бути без шкоди для інших зобов'язань суб'єктів розгортання стосовно систем ШІ з високим ризиком відповідно до права Союзу або національного права.

(92) Цей Регламент не завдає шкоди зобов'язанням роботодавців інформувати або інформувати та консультуватися з працівниками або їхніми представниками відповідно до права та практики Союзу та національного права, у тому числі Директиви Європейського Парламенту і Ради 2002/14/ЄС (39), щодо рішень про введення в експлуатацію або використання систем ШІ. Залишається необхідним забезпечення інформування працівників та їхніх представників про заплановане розгортання систем ШІ з високим ризиком на робочому місці там, де умови для таких зобов'язань з інформування або інформування та консультування за іншими правовими інструментами не виконуються. Крім того, таке право на інформацію є допоміжним та необхідним для досягнення мети захисту основоположних прав, що лежить в основі цього Регламенту. Тому у цьому Регламенті має бути встановлено вимогу щодо інформування з таким ефектом, без будь-якого впливу на існуючі права працівників.

(93) Хоча ризики, пов'язані із системами ШІ, можуть виникати внаслідок способу проектування таких систем, ризики також можуть виникати внаслідок того, як такі системи ШІ використовуються. Суб'єкти розгортання систем ШІ з високим ризиком тому відіграють вирішальну роль у забезпеченні захисту основоположних прав, доповнюючи зобов'язання провайдера при розробці системи ШІ. Суб'єкти розгортання найкраще обізнані про те, як система ШІ з високим ризиком конкретно використовуватиметься, і тому можуть виявляти потенційні значні ризики, що не були передбачені на етапі розробки, завдяки точнішому знанню контексту використання, осіб або груп осіб, що можуть зазнати впливу, у тому числі вразливих груп. Суб'єкти розгортання

систем ШІ з високим ризиком, перелічених у додатку до цього Регламенту, також відіграють вирішальну роль в інформуванні фізичних осіб та мають, коли вони приймають рішення або допомагають у прийнятті рішень, пов'язаних із фізичними особами, де застосовно, інформувати фізичних осіб про те, що вони є суб'єктами використання системи ШІ з високим ризиком. Ця інформація має включати призначену мету та тип рішень, які вона приймає. Суб'єкт розгортання також має інформувати фізичних осіб про їхнє право на роз'яснення, передбачене цим Регламентом. Щодо систем ШІ з високим ризиком, що використовуються у цілях правоохоронної діяльності, це зобов'язання має виконуватися відповідно до статті 13 Директиви (ЄС) 2016/680.

(94) Будь-яка обробка біометричних даних, що передбачається при використанні систем ШІ для біометричної ідентифікації у цілях правоохоронної діяльності, має відповідати статті 10 Директиви (ЄС) 2016/680, яка дозволяє таку обробку лише там, де це суворо необхідно, за умови відповідних гарантій прав і свобод суб'єкта даних та за наявності дозволу з боку права Союзу або держави-члена. Таке використання, якщо воно авторизоване, також має поважати принципи, встановлені у статті 4(1) Директиви (ЄС) 2016/680, у тому числі законність, справедливість та прозорість, обмеженість мети, точність та обмеженість зберігання.

(95) Без шкоди для застосовного права Союзу, зокрема Регламенту (ЄС) 2016/679 та Директиви (ЄС) 2016/680, враховуючи інтрузивний характер систем постфактичної дистанційної біометричної ідентифікації, використання систем постфактичної дистанційної біометричної ідентифікації має підпорядковуватися гарантіям. Системи постфактичної дистанційної біометричної ідентифікації мають завжди використовуватися пропорційним, законним та суворо необхідним способом і, таким чином, цілеспрямовано, стосовно осіб, що підлягають ідентифікації, місця розташування, часових меж та на основі закритого набору даних законно отриманих відеозаписів. У будь-якому разі

системи постфактичної дистанційної біометричної ідентифікації не мають використовуватися в рамках правоохоронної діяльності з метою невибіркового стеження. Умови для постфактичної дистанційної біометричної ідентифікації у будь-якому разі не мають надавати підстав для обходу умов заборони та суворих виключень для дистанційної біометричної ідентифікації в режимі реального часу.

(96) Для ефективного забезпечення захисту основоположних прав суб'єкти розгортання систем ШІ з високим ризиком, що є органами, керованими публічним правом, або приватними суб'єктами, що надають публічні послуги, та суб'єкти розгортання певних систем ШІ з високим ризиком, перелічених у додатку до цього Регламенту, наприклад банківські або страхові суб'єкти, мають проводити оцінку впливу на основоположні права до початку використання. Послуги, важливі для осіб, що мають публічний характер, також можуть надаватися приватними суб'єктами. Приватні суб'єкти, що надають такі публічні послуги, пов'язані із завданнями в суспільних інтересах, наприклад у сферах освіти, охорони здоров'я, соціальних послуг, житла, відправлення правосуддя. Метою оцінки впливу на основоположні права є виявлення суб'єктом розгортання конкретних ризиків для прав осіб або груп осіб, на яких, ймовірно, буде здійснено вплив, та визначення заходів, що вживаються у разі матеріалізації цих ризиків. Оцінка впливу має проводитися до розгортання системи ШІ з високим ризиком та має оновлюватися, коли суб'єкт розгортання вважає, що будь-який із відповідних чинників змінився. Оцінка впливу має ідентифікувати відповідні процеси суб'єкта розгортання, в яких система ШІ з високим ризиком використовуватиметься відповідно до її призначеної мети, та має включати опис проміжку часу та частоти, в яких система призначена до використання, а також конкретних категорій фізичних осіб та груп, які можуть зазнати впливу в конкретному контексті використання. Оцінка також має включати виявлення конкретних ризиків шкоди, здатних впливати на основоположні права цих осіб або

груп. Під час проведення цієї оцінки суб'єкт розгортання має враховувати інформацію, релевантну для належної оцінки впливу, у тому числі, але не лише, інформацію, надану провайдером системи ШІ з високим ризиком в інструкціях з використання. З огляду на виявлені ризики суб'єкти розгортання мають визначати заходи, що вживаються у разі матеріалізації цих ризиків, включаючи, наприклад, механізми управління в цьому конкретному контексті використання, такі як механізми нагляду з боку людини відповідно до інструкцій з використання або процедури розгляду скарг та відшкодування, оскільки вони можуть відіграти ключову роль у пом'якшенні ризиків для основоположних прав у конкретних варіантах використання. Після проведення цієї оцінки впливу суб'єкт розгортання має повідомляти відповідний орган ринкового нагляду. Де доречно, для збору відповідної інформації, необхідної для проведення оцінки впливу, суб'єкти розгортання систем ШІ з високим ризиком, зокрема коли системи ШІ використовуються в публічному секторі, можуть залучати відповідних зацікавлених сторін, у тому числі представників груп осіб, на яких, ймовірно, буде здійснено вплив від системи ШІ, незалежних експертів та організації громадянського суспільства до проведення таких оцінок впливу та розробки заходів, що вживаються у разі матеріалізації ризиків. Європейське управління з питань штучного інтелекту (Управління ШІ) має розробити шаблон анкети з метою сприяння дотриманню та зменшення адміністративного тягаря для суб'єктів розгортання.

(97) Поняття моделей ШІ загального призначення має бути чітко визначено та відмежовано від поняття систем ШІ для забезпечення правової визначеності. Визначення має ґрунтуватися на ключових функціональних характеристиках моделі ШІ загального призначення, зокрема на загальності та здатності компетентно виконувати широкий спектр різноманітних завдань. Ці моделі, як правило, навчаються на великих обсягах даних за допомогою різних методів, таких як самоконтрольоване, неконтрольоване або навчання з підкріпленням. Моделі ШІ

загального призначення можуть вводитися в обіг різними способами, у тому числі через бібліотеки, програмні інтерфейси застосунків (API), у вигляді прямого завантаження або фізичної копії. Ці моделі можуть бути далі модифіковані або донавчені до нових моделей. Хоча моделі ШІ є важливими компонентами систем ШІ, вони самі по собі не є системами ШІ. Моделям ШІ для перетворення на системи ШІ необхідне додавання подальших компонентів, наприклад інтерфейсу користувача. Моделі ШІ, як правило, інтегруються в системи ШІ та є їхньою частиною. Цей Регламент передбачає конкретні правила для моделей ШІ загального призначення та для моделей ШІ загального призначення, що становлять системні ризики, які мають застосовуватися також тоді, коли ці моделі інтегруються або є частиною системи ШІ. Має розумітися, що зобов'язання для провайдерів моделей ШІ загального призначення мають застосовуватися після введення моделей ШІ загального призначення в обіг. Коли провайдер моделі ШІ загального призначення інтегрує власну модель у власну систему ШІ, що надається в користування на ринку або вводиться в експлуатацію, та модель має вважатися введеною в обіг і тому зобов'язання у цьому Регламенті стосовно моделей мають продовжувати застосовуватися на додаток до тих, що стосуються систем ШІ. Зобов'язання, встановлені для моделей, у будь-якому разі не мають застосовуватися, коли власна модель використовується для суто внутрішніх процесів, що не є необхідними для надання продукту або послуги третім сторонам і права фізичних осіб не зачіпаються. З огляду на їхні потенційно значно негативні наслідки, моделі ШІ загального призначення із системним ризиком завжди мають підпорядковуватися відповідним зобов'язанням відповідно до цього Регламенту. Визначення не має охоплювати моделі ШІ, що використовуються до їхнього введення в обіг виключно з метою дослідницької, розробницької діяльності та створення прототипів. Це без шкоди для зобов'язання дотримуватися цього Регламенту, коли після такої діяльності модель вводиться в обіг.

(98) Хоча загальність моделі може, між іншим, також визначатися кількістю параметрів, моделі щонайменше з мільярдом параметрів, навчені на великому обсязі даних із використанням масштабного самоконтрольованого навчання, мають вважатися такими, що виявляють значну загальність та компетентно виконують широкий спектр різноманітних завдань.

(99) Великі генеративні моделі ШІ є типовим прикладом моделі ШІ загального призначення, оскільки вони дозволяють гнучко генерувати контент, наприклад у формі тексту, аудіо, зображень або відео, що може легко пристосовуватися до широкого спектру різноманітних завдань.

(100) Коли модель ШІ загального призначення інтегрується в систему ШІ або є її частиною, ця система має вважатися системою ШІ загального призначення, коли внаслідок цієї інтеграції ця система має здатність слугувати різноманітним цілям. Система ШІ загального призначення може використовуватися безпосередньо або може бути інтегрована в інші системи ШІ.

(101) Провайдери моделей ШІ загального призначення мають особливу роль та відповідальність у ланцюгу створення вартості ШІ, оскільки надані ними моделі можуть формувати основу для ряду систем нижчих ланок, часто надаваних провайдерами нижчих ланок, які вимагають хорошого розуміння моделей та їхніх можливостей — як для забезпечення інтеграції таких моделей у свої продукти, так і для виконання своїх зобов'язань відповідно до цього або інших регламентів. Тому мають бути встановлені пропорційні заходи прозорості, у тому числі складання та оновлення документації та надання інформації про модель ШІ загального призначення для її використання провайдерами нижчих ланок. Технічна документація має складатися та оновлюватися провайдером моделі ШІ загального призначення з метою надання її, на запит, Управлінню ШІ та національним компетентним органам. Мінімальний набір елементів, що підлягають включенню до такої документації, має встановлюватися у конкретних додатках до цього

Регламенту. Комісія має бути уповноважена вносити зміни до цих додатків за допомогою делегованих актів з огляду на технологічний розвиток.

(102) Програмне забезпечення та дані, у тому числі моделі, що поширюються відповідно до вільної ліцензії з відкритим вихідним кодом, яка дозволяє їх відкрито поширювати та де користувачі можуть вільно отримувати доступ до них, використовувати, модифікувати та перерозподіляти їх або їхні модифіковані версії, можуть сприяти дослідженням та інноваціям на ринку і надавати значні можливості для зростання для економіки Союзу. Моделі ШІ загального призначення, що поширюються за вільними ліцензіями з відкритим вихідним кодом, мають вважатися такими, що забезпечують високий рівень прозорості та відкритості, якщо їхні параметри, у тому числі ваги, інформація про архітектуру моделі та інформація про використання моделі є загальнодоступними. Ліцензія має також вважатися вільною та з відкритим вихідним кодом, коли вона дозволяє користувачам запускати, копіювати, розповсюджувати, вивчати, змінювати та вдосконалювати програмне забезпечення та дані, у тому числі моделі, за умови, що зазначається первісний провайдер моделі та дотримуються ідентичні або порівнянні умови розповсюдження.

(103) Вільні компоненти ШІ з відкритим вихідним кодом охоплюють програмне забезпечення та дані, у тому числі моделі та моделі ШІ загального призначення, інструменти, послуги або процеси системи ШІ. Вільні компоненти ШІ з відкритим вихідним кодом можуть надаватися через різні канали, у тому числі шляхом їхньої розробки у відкритих репозиторіях. Для цілей цього Регламенту компоненти ШІ, що надаються за плату або іншим чином монетизуються, у тому числі через надання технічної підтримки або інших послуг, у тому числі через програмну платформу, пов'язану з компонентом ШІ, або через використання персональних даних з причин, відмінних від виключно для підвищення безпеки, сумісності або інтероперабельності

програмного забезпечення, за винятком операцій між мікропідприємствами, не мають користуватися винятками, передбаченими для вільних компонентів ШІ з відкритим вихідним кодом. Сам по собі факт надання компонентів ШІ в доступ через відкриті репозиторії не має становити монетизацію.

(104) Провайдери моделей ШІ загального призначення, що поширюються за вільною ліцензією з відкритим вихідним кодом та чиї параметри, у тому числі ваги, інформація про архітектуру моделі та інформація про використання моделі, є загальнодоступними, мають підпорядковуватися виняткам стосовно вимог, пов'язаних із прозорістю, що застосовуються до моделей ШІ загального призначення, якщо тільки вони не можуть вважатися такими, що становлять системний ризик, у такому разі обставина, що модель є прозорою та супроводжується ліцензією з відкритим вихідним кодом, не має вважатися достатньою підставою для виключення дотримання зобов'язань відповідно до цього Регламенту. У будь-якому разі, враховуючи, що поширення моделей ШІ загального призначення за вільною ліцензією з відкритим вихідним кодом не обов'язково розкриває суттєву інформацію про набір даних, використаний для навчання або тонкого налаштування моделі, та про те, як при цьому забезпечувалося дотримання авторського права, виняток, передбачений для моделей ШІ загального призначення, від дотримання вимог, пов'язаних із прозорістю, не має стосуватися зобов'язання складати зведений огляд контенту, використаного для навчання моделі, та зобов'язання запровадити політику дотримання авторського права Союзу, зокрема виявлення та дотримання застереження про права відповідно до статті 4(3) Директиви Європейського Парламенту і Ради (ЄС) 2019/790 (40).

(105) Моделі ШІ загального призначення, зокрема великі генеративні моделі ШІ, здатні генерувати текст, зображення та інший контент, відкривають унікальні інноваційні можливості, але також становлять виклики для художників, авторів та

інших творців і для того, як їхній творчий контент створюється, розповсюджується, використовується та споживається. Розробка та навчання таких моделей вимагають доступу до величезних обсягів тексту, зображень, відео та інших даних. Методи видобутку тексту та даних можуть широко застосовуватися у цьому контексті для пошуку та аналізу такого контенту, який може охоронятися авторським правом та суміжними правами. Будь-яке використання контенту, захищеного авторським правом, вимагає дозволу відповідного правовласника, якщо тільки не застосовуються відповідні винятки та обмеження авторського права. Директива (ЄС) 2019/790 запровадила винятки та обмеження, що дозволяють відтворення та вилучення творів або інших об'єктів охорони з метою видобутку тексту та даних за певних умов. Відповідно до цих правил правовласники можуть вибрати збереження своїх прав на свої твори або інші об'єкти охорони для запобігання видобутку тексту та даних, якщо тільки це не здійснюється у цілях наукових досліджень. Якщо право відмовитися від участі було прямо застережено у відповідний спосіб, провайдери моделей ШІ загального призначення повинні отримати дозвіл від правовласників, якщо вони хочуть здійснювати видобуток тексту та даних із таких творів.

(106) Провайдери, що вводять моделі ШІ загального призначення в обіг на ринку Союзу, мають забезпечувати дотримання відповідних зобов'язань у цьому Регламенті. З цією метою провайдери моделей ШІ загального призначення мають запроваджувати політику дотримання права Союзу про авторське право та суміжні права, зокрема для виявлення та дотримання застереження про права, висловленого правовласниками відповідно до статті 4(3) Директиви (ЄС) 2019/790. Будь-який провайдер, що вводить модель ШІ загального призначення в обіг на ринку Союзу, має дотримуватися цього зобов'язання незалежно від юрисдикції, в якій відбуваються дії, що мають значення для авторського права, що лежать в основі навчання цих моделей ШІ загального призначення. Це необхідно для забезпечення рівних умов серед

провайдерів моделей ШІ загального призначення, де жоден провайдер не має мати можливості отримати конкурентну перевагу на ринку Союзу шляхом застосування нижчих стандартів авторського права, ніж ті, що передбачені в Союзі.

(107) З метою підвищення прозорості щодо даних, що використовуються під час попереднього навчання та навчання моделей ШІ загального призначення, у тому числі тексту та даних, захищених авторським правом, доцільно, щоб провайдери таких моделей складали та оприлюднювали достатньо детальний зведений огляд контенту, використаного для навчання моделі ШІ загального призначення. Беручи до уваги необхідність захисту комерційної таємниці та конфіденційної ділової інформації, цей зведений огляд має бути загалом вичерпним за своїм охопленням, а не технічно детальним, щоб допомогти сторонам із законними інтересами, у тому числі правовласникам, здійснювати та захищати свої права відповідно до права Союзу, наприклад шляхом переліку основних зібрань або наборів даних, що увійшли до навчання моделі, таких як великі приватні або публічні бази даних або архіви даних, та шляхом надання описового пояснення про інші використані джерела даних. Доцільно, щоб Управління ШІ надавало шаблон для зведеного огляду, який має бути простим, дієвим та дозволяти провайдеру надавати необхідний зведений огляд у описовій формі.

(108) Щодо зобов'язань, покладених на провайдерів моделей ШІ загального призначення щодо запровадження політики дотримання авторського права Союзу та оприлюднення зведеного огляду контенту, використаного для навчання, Управління ШІ має здійснювати моніторинг того, чи виконав провайдер ці зобов'язання, не перевіряючи та не переходячи до оцінки навчальних даних твір за твором з точки зору дотримання авторського права. Цей Регламент не впливає на правозастосування норм авторського права, передбачених правом Союзу.

(109) Дотримання зобов'язань, застосовних до провайдерів моделей ШІ загального призначення, має бути сумірним і пропорційним до типу провайдера моделі, виключаючи необхідність дотримання для осіб, які розробляють або використовують моделі у непрофесійних або наукових дослідницьких цілях, яких, тим не менш, слід заохочувати до добровільного дотримання цих вимог. Без шкоди для авторського права Союзу дотримання цих зобов'язань має належним чином враховувати розмір провайдера та дозволяти спрощені способи дотримання для МСП, у тому числі стартапів, що не мають становити надмірних витрат та не стримувати використання таких моделей. У разі модифікації або тонкого налаштування моделі зобов'язання для провайдерів моделей ШІ загального призначення мають обмежуватися цією модифікацією або тонким налаштуванням, наприклад шляхом доповнення вже існуючої технічної документації інформацією про модифікації, у тому числі нові джерела навчальних даних, як засіб дотримання зобов'язань у ланцюгу створення вартості, передбачених у цьому Регламенті.

(110) Моделі ШІ загального призначення можуть становити системні ризики, що включають, але не обмежуються, будь-якими фактичними або розумно передбачуваними негативними наслідками стосовно великих аварій, порушень роботи критичних секторів та серйозних наслідків для громадського здоров'я та безпеки; будь-якими фактичними або розумно передбачуваними негативними наслідками для демократичних процесів, публічної та економічної безпеки; поширенням незаконного, хибного або дискримінаційного контенту. Системні ризики мають розумітися як такі, що зростають разом із можливостями моделі та охопленням моделі, можуть виникати протягом усього життєвого циклу моделі та перебувають під впливом умов неналежного використання, надійності моделі, справедливості моделі та безпеки моделі, рівня автономії моделі, її доступу до інструментів, нових або комбінованих модальностей, стратегій випуску та

розповсюдження, потенціалу зняття захисних обмежень та інших чинників. Зокрема, міжнародні підходи наразі визначили необхідність приділяти увагу ризикам від потенційного навмисного неналежного використання або ненавмисних проблем контролю, пов'язаних із узгодженістю з людськими намірами; хімічним, біологічним, радіологічним та ядерним ризикам, наприклад тому, як можуть знижуватися бар'єри для входу, у тому числі для розробки, придбання схем або використання зброї; наступальним кіберможливостям, наприклад тому, як може бути забезпечено виявлення вразливостей, їхню експлуатацію або оперативне використання; наслідкам взаємодії та використання інструментів, у тому числі, наприклад, здатності управляти фізичними системами та втручатися в критичну інфраструктуру; ризикам від створення моделями копій себе або «самовідтворення» або навчання інших моделей; тому, як моделі можуть спричиняти шкідливу упередженість та дискримінацію з ризиками для осіб, спільнот або суспільств; сприянню дезінформації або заподіянню шкоди конфіденційності із загрозами демократичним цінностям та правам людини; ризику того, що конкретна подія може призвести до ланцюгової реакції зі значними негативними наслідками, що можуть вплинути на ціле місто, цілу галузь діяльності або цілу спільноту.

(111) Доцільно встановити методологію класифікації моделей ШІ загального призначення як моделей ШІ загального призначення із системними ризиками. Оскільки системні ризики є результатом особливо високих можливостей, модель ШІ загального призначення має вважатися такою, що становить системні ризики, якщо вона має можливості з великим впливом, що оцінюються на основі відповідних технічних інструментів та методологій, або значний вплив на внутрішній ринок завдяки своєму охопленню. Можливості з великим впливом у моделях ШІ загального призначення означають можливості, що відповідають або перевищують можливості, зафіксовані в найбільш передових моделях ШІ загального призначення. Повний спектр можливостей моделі може бути краще

зрозумілий після її введення в обіг або коли суб'єкти розгортання взаємодіють із моделлю. Відповідно до сучасного стану розвитку технологій на момент набрання чинності цим Регламентом, сукупний обсяг обчислень, використаних для навчання моделі ШІ загального призначення, що вимірюється операціями з плаваючою комою, є одним із відповідних наближень для можливостей моделі. Сукупний обсяг обчислень, використаних для навчання, включає обчислення, використані в рамках заходів і методів, призначених для підвищення можливостей моделі до розгортання, таких як попереднє навчання, генерація синтетичних даних та тонке налаштування. Тому має бути встановлено початковий поріг операцій з плаваючою комою, який у разі його досягнення моделлю ШІ загального призначення призводить до презумпції того, що модель є моделлю ШІ загального призначення із системними ризиками. Цей поріг має корегуватися з часом для відображення технологічних та промислових змін, таких як алгоритмічні вдосконалення або підвищення ефективності апаратного забезпечення, та має доповнюватися еталонами та показниками для оцінки можливостей моделі. Для інформування цього Управління ШІ має взаємодіяти з науковою спільнотою, промисловістю, громадянським суспільством та іншими експертами. Пороги, а також інструменти та еталони для оцінки можливостей з великим впливом мають бути надійними предикторами загальності, її можливостей та пов'язаного системного ризику моделей ШІ загального призначення і можуть враховувати спосіб введення моделі в обіг або кількість користувачів, на яких вона може вплинути. На доповнення цієї системи має існувати можливість для Комісії приймати індивідуальні рішення про призначення моделі ШІ загального призначення моделлю ШІ загального призначення із системним ризиком, якщо буде встановлено, що така модель має можливості або вплив, еквівалентні тим, що охоплені встановленим порогом. Це рішення має прийматися на основі загальної оцінки критеріїв призначення моделі ШІ загального призначення із системним ризиком, встановлених у додатку до цього

Регламенту, таких як якість або розмір навчального набору даних, кількість ділових і кінцевих користувачів, її вхідні та вихідні модальності, її рівень автономії та масштабованості або інструменти, до яких вона має доступ. На обґрунтований запит провайдера, чиєю моделлю було призначено модель ШІ загального призначення із системним ризиком, Комісія має враховувати запит та може вирішити переоцінити, чи може модель ШІ загального призначення й надалі вважатися такою, що становить системні ризики.

(112) Також необхідно уточнити процедуру класифікації моделі ШІ загального призначення із системними ризиками. Має презюмуватися, що модель ШІ загального призначення, що відповідає застосовному порогу для можливостей з великим впливом, є моделлю ШІ загального призначення із системним ризиком. Провайдер має повідомляти Управління ШІ не пізніше ніж через два тижні після виконання вимог або після того, як стає відомо, що модель ШІ загального призначення відповідатиме вимогам, що призводять до презумпції. Це особливо актуально стосовно порогу операцій з плаваючою комою, оскільки навчання моделей ШІ загального призначення вимагає значного планування, яке включає попереднє виділення обчислювальних ресурсів, і тому провайдери моделей ШІ загального призначення здатні знати, чи відповідатиме їхня модель порогу до завершення навчання. У контексті цього повідомлення провайдер має мати можливість демонструвати, що, з огляду на свої специфічні характеристики, модель ШІ загального призначення як виняток не становить системних ризиків і тому не має класифікуватися як модель ШІ загального призначення із системними ризиками. Ця інформація є цінною для Управління ШІ для передбачення введення в обіг моделей ШІ загального призначення із системними ризиками, і провайдери можуть починати взаємодіяти з Управлінням ШІ на ранньому етапі. Ця інформація є особливо важливою щодо моделей ШІ загального призначення, що плануються до випуску як моделі з відкритим вихідним кодом, враховуючи, що після випуску

моделі з відкритим вихідним кодом необхідні заходи для забезпечення дотримання зобов'язань відповідно до цього Регламенту можуть бути важчими для впровадження.

(113) Якщо Комісії стає відомо про те, що модель ШІ загального призначення відповідає вимогам для класифікації як моделі ШІ загального призначення із системним ризиком, що раніше або не було відомо, або про що відповідний провайдер не повідомив Комісію, Комісія має бути уповноважена здійснити таке призначення. Система кваліфікованих сповіщень має забезпечити, щоб Управління ШІ було поінформоване науковою панеллю про моделі ШІ загального призначення, які, можливо, мають класифікуватися як моделі ШІ загального призначення із системним ризиком, на доповнення до наглядових заходів Управління ШІ.

(114) Провайдери моделей ШІ загального призначення, що становлять системні ризики, мають підпорядковуватися, на додаток до зобов'язань, передбачених для провайдерів моделей ШІ загального призначення, зобов'язанням, спрямованим на виявлення та пом'якшення цих ризиків та забезпечення належного рівня захисту кібербезпеки, незалежно від того, чи вона надається як автономна модель або вбудована в систему ШІ або продукт. Для досягнення цих цілей цей Регламент має вимагати від провайдерів проведення необхідних оцінок моделей, зокрема до першого введення в обіг, у тому числі проведення та документування змагального тестування моделей, а також, де доречно, через внутрішнє або незалежне зовнішнє тестування. Крім того, провайдери моделей ШІ загального призначення із системними ризиками мають безперервно оцінювати та пом'якшувати системні ризики, у тому числі, наприклад, шляхом запровадження політик управління ризиками, таких як процеси підзвітності та управління, впровадження моніторингу після введення в обіг, вжиття відповідних заходів протягом усього

життєвого циклу моделі та співпраці з відповідними суб'єктами у ланцюгу створення вартості ШІ.

(115) Провайдери моделей ШІ загального призначення із системними ризиками мають оцінювати та пом'якшувати можливі системні ризики. Якщо, незважаючи на зусилля з виявлення та запобігання ризикам, пов'язаним із моделлю ШІ загального призначення, що може становити системні ризики, розробка або використання моделі спричиняє серйозний інцидент, провайдер моделі ШІ загального призначення має без невиправданої затримки відстежувати інцидент та повідомляти Комісії та національним компетентним органам будь-яку відповідну інформацію та можливі коригувальні заходи. Крім того, провайдери мають забезпечувати належний рівень захисту кібербезпеки для моделі та її фізичної інфраструктури, де доречно, протягом усього життєвого циклу моделі. Захист кібербезпеки, пов'язаний із системними ризиками, пов'язаними зі зловмисним використанням або атаками, має належним чином враховувати випадковий витік моделі, несанкціоновані випуски, обхід захисних заходів та захист від кібератак, несанкціонованого доступу або крадіжки моделі. Такий захист може забезпечуватися шляхом захисту ваг моделі, алгоритмів, серверів та наборів даних, наприклад за допомогою оперативних заходів безпеки для інформаційної безпеки, конкретних політик кібербезпеки, адекватних технічних та усталених рішень, а також засобів контролю кібернетичного та фізичного доступу, відповідних відповідним обставинам та залученим ризикам.

(116) Управління ШІ має заохочувати та сприяти складанню, перегляду та адаптації кодексів практики з урахуванням міжнародних підходів. Усі провайдери моделей ШІ загального призначення можуть бути запрошені до участі. Для забезпечення того, щоб кодекси практики відображали сучасний стан розвитку технологій та належним чином враховували різноманітний набір точок зору, Управління ШІ має співпрацювати з відповідними національними

компетентними органами та може, де доречно, консультуватися з організаціями громадянського суспільства та іншими відповідними зацікавленими сторонами та експертами, у тому числі Науковою панеллю, для складання таких кодексів. Кодекси практики мають охоплювати зобов'язання для провайдерів моделей ШІ загального призначення та моделей ШІ загального призначення, що становлять системні ризики. Крім того, стосовно системних ризиків кодекси практики мають сприяти встановленню таксономії ризиків типу та характеру системних ризиків на рівні Союзу, у тому числі їхніх джерел. Кодекси практики також мають бути зосереджені на конкретних заходах оцінки ризиків та їх пом'якшення.

(117) Кодекси практики мають становити центральний інструмент для належного дотримання зобов'язань, передбачених у цьому Регламенті для провайдерів моделей ШІ загального призначення. Провайдери мають мати можливість спиратися на кодекси практики для демонстрації дотримання зобов'язань. За допомогою виконавчих актів Комісія може вирішити затвердити кодекс практики та надати йому загальну чинність у межах Союзу або, альтернативно, забезпечити загальні правила виконання відповідних зобов'язань, якщо на момент початку застосування цього Регламенту кодекс практики не може бути завершений або не вважається Управлінням ШІ адекватним. Після публікації гармонізованого стандарту та його оцінки Управлінням ШІ як такого, що підходить для охоплення відповідних зобов'язань, дотримання Європейського гармонізованого стандарту має надавати провайдерам презумпцію відповідності. Провайдери моделей ШІ загального призначення також мають мати можливість демонструвати дотримання за допомогою альтернативних адекватних засобів, якщо кодекси практики або гармонізовані стандарти не є доступними, або вони вирішують не спиратися на них.

(118) Цей Регламент регулює системи ШІ та моделі ШІ шляхом встановлення певних вимог і зобов'язань для відповідних ринкових суб'єктів, що вводять їх

в обіг, в експлуатацію або використовують у Союзі, таким чином доповнюючи зобов'язання для провайдерів посередницьких послуг, що вбудовують такі системи або моделі у свої послуги, що регулюються Регламентом (ЄС) 2022/2065. Тою мірою, якою такі системи або моделі вбудовані в призначені дуже великі онлайн-платформи або дуже великі пошукові системи в інтернеті, вони підпорядковуються системі управління ризиками, передбаченій Регламентом (ЄС) 2022/2065. Відповідно, відповідні зобов'язання цього Регламенту мають вважатися виконаними, якщо тільки в таких моделях не виникають та не виявляються значні системні ризики, не охоплені Регламентом (ЄС) 2022/2065. У цих рамках провайдери дуже великих онлайн-платформ та дуже великих пошукових систем в інтернеті зобов'язані оцінювати потенційні системні ризики, що випливають із дизайну, функціонування та використання їхніх послуг, у тому числі те, як дизайн алгоритмічних систем, що використовуються в послузі, може сприяти таким ризикам, а також системні ризики, що випливають із потенційних видів неналежного використання. Ці провайдери також зобов'язані вживати відповідних пом'якшувальних заходів з дотриманням основоположних прав.

(119) Враховуючи швидкий темп інновацій та технологічну еволюцію цифрових послуг у сфері дії різних інструментів права Союзу, зокрема маючи на увазі використання та сприйняття їхніми одержувачами, системи ШІ, що підпадають під дію цього Регламенту, можуть надаватися як посередницькі послуги або їхні частини у значенні Регламенту (ЄС) 2022/2065, який має тлумачитися в технологічно нейтральний спосіб. Наприклад, системи ШІ можуть використовуватися для надання пошукових систем в інтернеті, зокрема тою мірою, якою система ШІ, наприклад онлайн-чатбот, здійснює пошуки, в принципі, на всіх веб-сайтах, потім включає результати до своїх існуючих знань та використовує оновлені знання для генерування єдиного вихідного результату, що поєднує різні джерела інформації.

(120) Крім того, зобов'язання, покладені на провайдерів та суб'єктів розгортання певних систем ШІ у цьому Регламенті, щодо забезпечення можливості виявлення та розкриття того, що вихідні дані цих систем штучно генеруються або маніпулюються, є особливо актуальними для сприяння ефективному виконанню Регламенту (ЄС) 2022/2065. Це застосовується зокрема щодо зобов'язань провайдерів дуже великих онлайн-платформ або дуже великих пошукових систем в інтернеті виявляти та пом'якшувати системні ризики, що можуть виникати внаслідок поширення штучно генерованого або маніпульованого контенту, зокрема ризику фактичних або передбачуваних негативних наслідків для демократичних процесів, громадянського дискурсу та виборчих процесів, у тому числі через дезінформацію.

(121) Стандартизація має відігравати ключову роль у наданні технічних рішень постачальникам для забезпечення відповідності цьому Регламенту згідно з рівнем розвитку техніки, а також для сприяння інноваціям, конкурентоспроможності та зростанню на єдиному ринку. Відповідність гармонізованим стандартам, як це визначено в статті 2, пункт (1)(c), Регламенту (ЄС) № 1025/2012 Європейського Парламенту і Ради (41), які зазвичай мають відображати рівень розвитку техніки, повинні бути засобом для постачальників демонструвати відповідність вимогам цього Регламенту. Слід заохочувати збалансоване представництво інтересів усіх відповідних зацікавлених сторін у розробці стандартів, зокрема МСП, організацій споживачів та екологічних і соціальних зацікавлених сторін відповідно до статей 5 та 6 Регламенту (ЄС) № 1025/2012. З метою полегшення забезпечення відповідності запити на стандартизацію повинні надаватися Комісією без невиправданих затримок. При підготовці запиту на стандартизацію Комісія повинна консультуватися з дорадчим форумом та Радою з метою збору відповідної експертизи. Однак за відсутності відповідних посилань на гармонізовані стандарти Комісія повинна мати можливість встановлювати через

імплементаційні акти та після консультації з дорадчим форумом загальні специфікації для певних вимог відповідно до цього Регламенту. Загальна специфікація має бути виключним резервним рішенням для полегшення зобов'язання постачальника дотримуватися вимог цього Регламенту у випадках, коли запит на стандартизацію не було прийнято жодною з європейських організацій зі стандартизації, або коли відповідні гармонізовані стандарти недостатньо враховують проблеми основних прав, або коли гармонізовані стандарти не відповідають запиту, або коли існують затримки у прийнятті відповідного гармонізованого стандарту. Якщо така затримка у прийнятті гармонізованого стандарту обумовлена технічною складністю цього стандарту, Комісія повинна брати до уваги цей факт перед тим, як розглядати питання встановлення загальних специфікацій. При розробці загальних специфікацій Комісія заохочується до співпраці з міжнародними партнерами та міжнародними органами зі стандартизації.

(122) Доречно, щоб без шкоди для використання гармонізованих стандартів і загальних специфікацій постачальники високоризикованих систем ШІ, які пройшли навчання та тестування на даних, що відображають конкретне географічне, поведінкове, контекстуальне або функціональне середовище, в якому передбачається використовувати систему ШІ, вважалися такими, що відповідають відповідному заходу, передбаченому вимогою щодо управління даними, встановленою цим Регламентом. Без шкоди для вимог щодо стійкості та точності, встановлених цим Регламентом, відповідно до статті 54(3) Регламенту (ЄС) 2019/881, високоризиковані системи ШІ, які отримали сертифікат або для яких видано заяву про відповідність відповідно до схеми кібербезпеки згідно з тим Регламентом, і посилання на які опубліковані в Офіційному журналі Європейського Союзу вважаються такими, що відповідають вимозі кібербезпеки цього Регламенту, тією мірою, якою сертифікат кібербезпеки або заява про відповідність чи їх частини охоплюють вимогу кібербезпеки цього

Регламенту. Це залишається без шкоди для добровільного характеру зазначеної схеми кібербезпеки.

(123) З метою забезпечення високого рівня надійності високоризикованих систем ШІ такі системи повинні підлягати оцінці відповідності до їх розміщення на ринку або введення в експлуатацію.

(124) Доречно, щоб з метою мінімізації навантаження на операторів та уникнення будь-якого можливого дублювання для високоризикованих систем ШІ, пов'язаних з продуктами, на які поширюється чинне гармонізаційне законодавство Союзу, засноване на Новій законодавчій базі, відповідність цих систем ШІ вимогам цього Регламенту оцінювалася в рамках оцінки відповідності, вже передбаченої таким законодавством. Таким чином, застосовність вимог цього Регламенту не повинна впливати на конкретну логіку, методологію або загальну структуру оцінки відповідності згідно з відповідним гармонізаційним законодавством Союзу.

(125) З огляду на складність високоризикованих систем ШІ та пов'язані з ними ризики важливо розробити належну процедуру оцінки відповідності для таких систем із залученням нотифікованих органів — так звану оцінку відповідності третьою стороною. Однак, зважаючи на нинішній досвід професійних попередніх ринкових сертифікаторів у сфері безпеки продуктів та різний характер пов'язаних ризиків, доречно обмежити — принаймні на початковому етапі застосування цього Регламенту — сферу застосування оцінки відповідності третьою стороною для високоризикованих систем ШІ, що не пов'язані з продуктами. Тому оцінку відповідності таких систем як загальне правило повинен проводити постачальник під власну відповідальність, з єдиним винятком для систем ШІ, призначених для використання у сфері біометрії.

(126) З метою проведення оцінок відповідності третьою стороною, коли це потрібно, нотифіковані органи повинні бути нотифіковані

відповідно до цього Регламенту національними компетентними органами за умови, що вони відповідають низці вимог, зокрема щодо незалежності, компетентності, відсутності конфліктів інтересів та відповідних вимог кібербезпеки. Повідомлення про такі органи повинні надсилатися національними компетентними органами до Комісії та інших держав-членів за допомогою електронного інструменту повідомлення, розробленого та управління яким здійснюється Комісією відповідно до статті R23 Додатка I до Рішення № 768/2008/ЄС.

(127) Відповідно до зобов'язань Союзу за Угодою Світової організації торгівлі про технічні бар'єри в торгівлі доцільно сприяти взаємному визнанню результатів оцінки відповідності, що виготовляються компетентними органами оцінки відповідності, незалежно від території, на якій вони розташовані, за умови, що органи оцінки відповідності, засновані за законодавством третьої країни, відповідають застосовним вимогам цього Регламенту та Союз уклав відповідну угоду. У цьому контексті Комісія повинна активно вивчати можливі міжнародні інструменти для досягнення цієї мети та зокрема прагнути до укладення угод про взаємне визнання з третіми країнами.

(128) Відповідно до загальновизнаного поняття суттєвої модифікації для продуктів, що регулюються гармонізаційним законодавством Союзу, доречно, щоб при виникненні будь-яких змін, які можуть вплинути на відповідність високоризикованої системи ШІ цьому Регламенту (наприклад, зміна операційної системи або програмної архітектури) або при зміні передбаченого призначення системи, така система ШІ вважалася новою системою ШІ, яка повинна пройти нову оцінку відповідності. Однак зміни алгоритму та продуктивності систем ШІ, які продовжують «навчатися» після розміщення на ринку або введення в експлуатацію, тобто автоматично адаптують спосіб виконання функцій, не повинні становити суттєву

модифікацію за умови, що ці зміни були попередньо визначені постачальником та оцінені на момент проведення оцінки відповідності.

(129) Високоризиковані системи ШІ повинні мати маркування CE для позначення їх відповідності цьому Регламенту, щоб вони могли вільно переміщатися на внутрішньому ринку. Для високоризикованих систем ШІ, вбудованих у продукт, має бути нанесено фізичне маркування CE, яке може доповнюватися цифровим маркуванням CE. Для високоризикованих систем ШІ, що надаються виключно в цифровому вигляді, повинно використовуватися цифрове маркування CE. Держави-члени не повинні створювати невиправданих перешкод для розміщення на ринку або введення в експлуатацію високоризикованих систем ШІ, які відповідають вимогам, встановленим цим Регламентом, та мають маркування CE.

(130) За певних умов швидка доступність інноваційних технологій може мати вирішальне значення для здоров'я та безпеки осіб, захисту навколишнього середовища та клімату, а також для суспільства в цілому. Тому доречно, щоб за виняткових підстав суспільної безпеки або захисту життя та здоров'я фізичних осіб, охорони навколишнього середовища та захисту ключових промислових і інфраструктурних активів органи ринкового нагляду могли дозволяти розміщення на ринку або введення в експлуатацію систем ШІ, які не пройшли оцінку відповідності. У належно обґрунтованих ситуаціях, передбачених цим Регламентом, правоохоронні органи або органи цивільного захисту можуть вводити в експлуатацію конкретну високоризиковану систему ШІ без дозволу органу ринкового нагляду за умови, що такий дозвіл запитується під час або після використання без невиправданої затримки.

(131) З метою полегшення роботи Комісії та держав-членів у сфері ШІ, а також підвищення прозорості для громадськості постачальники високоризикованих систем ШІ, відмінних від тих, що пов'язані з продуктами, що підпадають під сферу застосування відповідного чинного гармонізаційного законодавства Союзу, а також

постачальники, які вважають, що система ШІ, включена до переліку випадків використання з високим ризиком у додатку до цього Регламенту, не є високоризикованою на підставі відступу, повинні бути зобов'язані реєструвати себе та інформацію про свою систему ШІ в базі даних ЄС, що має бути створена та управлятися Комісією. Перед використанням системи ШІ, включеної до переліку випадків використання з високим ризиком у додатку до цього Регламенту, суб'єкти розгортання високоризикованих систем ШІ, які є органами публічної влади, агентствами або органами, повинні реєструватися в такій базі даних та обирати систему, яку вони мають намір використовувати. Інші суб'єкти розгортання повинні мати право робити це добровільно. Цей розділ бази даних ЄС має бути загальнодоступним та безкоштовним, інформація в ньому має бути легкою для навігації, зрозумілою та машинозчитуваною. База даних ЄС також має бути зручною для користувачів, наприклад шляхом надання функцій пошуку, зокрема за ключовими словами, що дозволяє широкій громадськості знаходити відповідну інформацію, що має надаватися при реєстрації високоризикованих систем ШІ та про випадки використання високоризикованих систем ШІ, зазначені в додатку до цього Регламенту, яким відповідають такі системи ШІ. Будь-яка суттєва модифікація високоризикованих систем ШІ також має реєструватися в базі даних ЄС. Для високоризикованих систем ШІ у сфері правоохоронної діяльності, міграції, притулку та управління кордонами реєстраційні зобов'язання повинні виконуватися в захищеному непублічному розділі бази даних ЄС. Доступ до захищеного непублічного розділу має бути суворо обмежений Комісією, а також органами ринкового нагляду щодо їхнього національного розділу цієї бази даних. Високоризикові системи ШІ у сфері критичної інфраструктури реєструються лише на національному рівні. Комісія має бути контролером бази даних ЄС відповідно до Регламенту (ЄС) 2018/1725. З метою забезпечення повної функціональності бази даних ЄС після її розгортання процедура налаштування бази даних має включати

розробку функціональних специфікацій Комісією та незалежний аудиторський звіт. Комісія повинна враховувати ризики кібербезпеки при виконанні своїх завдань як контролера даних бази даних ЄС. З метою максимізації доступності та використання бази даних ЄС громадськістю база даних ЄС, включаючи інформацію, доступну через неї, має відповідати вимогам Директиви (ЄС) 2019/882.

(132) Певні системи ШІ, призначені для взаємодії з фізичними особами або для створення контенту, можуть становити особливі ризики самозванства або обману, незалежно від того, чи класифікуються вони як системи з високим ризиком. У певних обставинах використання таких систем повинно тому підлягати конкретним зобов'язанням щодо прозорості без шкоди для вимог та зобов'язань для високоризикованих систем ШІ, а також з урахуванням цілеспрямованих винятків для врахування особливих потреб правоохоронних органів. Зокрема, фізичні особи повинні отримувати повідомлення про те, що вони взаємодіють із системою ШІ, якщо це не є очевидним з точки зору достатньо поінформованої, уважної та обачної фізичної особи з урахуванням обставин та контексту використання. При виконанні цього зобов'язання слід враховувати характеристики фізичних осіб, які належать до вразливих груп через вік або інвалідність, тією мірою, якою система ШІ призначена для взаємодії з такими групами. Крім того, фізичних осіб слід повідомляти у випадках, коли вони зазнають впливу систем ШІ, які шляхом обробки їхніх біометричних даних можуть ідентифікувати або виводити їхні емоції чи наміри або відносити їх до конкретних категорій. Такі конкретні категорії можуть стосуватися таких аспектів, як стать, вік, колір волосся, колір очей, татуювання, особисті риси, етнічне походження, особисті уподобання та інтереси. Така інформація та повідомлення повинні надаватися у доступних форматах для осіб з інвалідністю.

(133)

Різноманітні системи ШІ можуть генерувати великі обсяги синтетичного контенту, який людям стає дедалі важче відрізнити від контенту, створеного людиною, та автентичного контенту. Широка доступність і зростаючі можливості таких систем мають значний вплив на цілісність та довіру до інформаційної екосистеми, породжуючи нові ризики дезінформації та маніпуляцій у масштабі, шахрайства, самозванства та обману споживачів. З огляду на ці наслідки, швидкий технологічний прогрес та потребу в нових методах і техніках відстеження походження інформації, доречно вимагати від постачальників таких систем впроваджувати технічні рішення, що дозволяють маркування в машинозчитуваному форматі та виявлення того, що вихідні дані були згенеровані або маніпульовані системою ШІ, а не людиною. Такі техніки та методи повинні бути достатньо надійними, сумісними, ефективними та стійкими, наскільки це технічно можливо, з урахуванням доступних технік або комбінації таких технік, як водяні знаки, ідентифікація метаданих, криптографічні методи для підтвердження походження та автентичності контенту, методи журналювання, цифрові відбитки або інші техніки, залежно від обставин. При виконанні цього зобов'язання постачальники також повинні враховувати особливості та обмеження різних типів контенту та відповідні технологічні та ринкові розробки в цій сфері, відображені в загальновизнаному рівні розвитку техніки. Такі техніки та методи можуть впроваджуватися на рівні системи ШІ або на рівні моделі ШІ, включаючи загальноцільові моделі ШІ, що генерують контент, тим самим полегшуючи виконання цього зобов'язання постачальником системи ШІ нижчої ланки. Для збереження пропорційності доречно передбачити, що це зобов'язання маркування не повинно поширюватися на системи ШІ, що виконують переважно допоміжну функцію для стандартного редагування, або системи ШІ, що не суттєво змінюють вхідні дані, надані суб'єктом розгортання, або їх семантику.

(134) На додаток до технічних рішень, що застосовуються постачальниками системи ШІ, суб'єкти розгортання, які використовують систему ШІ для створення або маніпулювання зображеннями, аудіо або відеовмістом, що помітно схожий на реальних осіб, об'єкти, місця, суб'єкти або події та міг би помилково здатися особі автентичним або правдивим (дипфейки), також повинні чітко та виразно розкривати, що контент був штучно створений або маніпульований, відповідно маркуючи вихідні дані ШІ та розкриваючи їх штучне походження. Виконання цього зобов'язання щодо прозорості не повинно тлумачитися як вказівка на те, що використання системи ШІ або її вихідних даних перешкоджає праву на свободу вираження поглядів та праву на свободу мистецтва та науки, гарантованих Хартією, зокрема там, де контент є частиною явно творчого, сатиричного, художнього, вигаданого або аналогічного твору або програми, з урахуванням відповідних гарантій прав та свобод третіх осіб. У таких випадках зобов'язання щодо прозорості для дипфейків, встановлене цим Регламентом, обмежується розкриттям існування такого створеного або маніпульованого контенту у відповідний спосіб, що не заважає демонстрації або отриманню задоволення від твору, включаючи його нормальне використання, при збереженні корисності та якості твору. Крім того, доречно передбачити аналогічне зобов'язання щодо розкриття стосовно тексту, створеного або маніпульованого ШІ, тією мірою, якою він публікується з метою інформування громадськості з питань суспільного інтересу, якщо контент, створений ШІ, не пройшов процес перегляду людиною або редакційного контролю та якщо фізична або юридична особа несе редакційну відповідальність за публікацію контенту.

(135) Без шкоди для обов'язкового характеру та повної застосовності зобов'язань щодо прозорості Комісія може також заохочувати та сприяти розробці кодексів практики на рівні Союзу для полегшення ефективного виконання зобов'язань щодо виявлення та маркування штучно створеного або маніпульованого контенту,

включаючи підтримку практичних заходів для забезпечення доступності, де це доречно, механізмів виявлення та сприяння співпраці з іншими учасниками ланцюжка цінностей, поширення контенту або перевірки його автентичності та походження, щоб громадськість могла ефективно розрізняти контент, створений ШІ.

(136) Зобов'язання, покладені цим Регламентом на постачальників та суб'єктів розгортання певних систем ШІ з метою забезпечення виявлення та розкриття того, що вихідні дані таких систем штучно створені або маніпульовані, є особливо актуальними для сприяння ефективному виконанню Регламенту (ЄС) 2022/2065. Це стосується зокрема зобов'язань постачальників дуже великих онлайн-платформ або дуже великих онлайн-пошукових систем щодо виявлення та пом'якшення системних ризиків, що можуть виникати внаслідок поширення контенту, який був штучно створений або маніпульований, зокрема ризику фактичних або передбачуваних негативних наслідків для демократичних процесів, громадянського дискурсу та виборчих процесів, включаючи через дезінформацію. Вимога щодо маркування контенту, створеного системами ШІ відповідно до цього Регламенту, не завдає шкоди зобов'язанню, передбаченому статтею 16(6) Регламенту (ЄС) 2022/2065, для постачальників хостингових послуг щодо обробки повідомлень про незаконний контент, отриманих відповідно до статті 16(1) зазначеного Регламенту, та не повинна впливати на оцінку та рішення щодо незаконності конкретного контенту. Така оцінка має здійснюватися виключно з посиланням на правила, що регулюють законність контенту.

(137) Виконання зобов'язань щодо прозорості для систем ШІ, що охоплюються цим Регламентом, не повинно тлумачитися як вказівка на те, що використання системи ШІ або її вихідних даних є законним відповідно до цього Регламенту або іншого законодавства Союзу та держав-членів, та має бути без шкоди для інших зобов'язань щодо

прозорості для суб'єктів розгортання систем ШІ, встановлених законодавством Союзу або національним законодавством.

(138) ШІ — це технологічна сім'я, що швидко розвивається та потребує регуляторного нагляду та безпечного та контрольованого простору для експериментів, забезпечуючи при цьому відповідальні інновації та інтеграцію відповідних захисних заходів та заходів із зменшення ризиків. Для забезпечення правової бази, що сприяє інноваціям, є перспективною та стійкою до збоїв, держави-члени повинні забезпечити, щоб їхні національні компетентні органи створили принаймні один регуляторний пісочниця ШІ на національному рівні для полегшення розробки та тестування інноваційних систем ШІ під суворим регуляторним наглядом до розміщення таких систем на ринку або введення їх в експлуатацію іншим чином. Держави-члени також можуть виконати це зобов'язання через участь у вже існуючих регуляторних пісочницях або спільне створення пісочниці з одним або кількома компетентними органами держав-членів, тією мірою, якою така участь забезпечує еквівалентний рівень національного охоплення для держав-членів, що беруть участь. Регуляторні пісочниці ШІ можуть створюватися у фізичній, цифровій або гібридній формі та можуть включати як фізичні, так і цифрові продукти. Органи, що створюють пісочниці, також повинні забезпечити наявність у регуляторних пісочницях ШІ достатніх ресурсів для їхнього функціонування, включаючи фінансові та людські ресурси.

(139) Цілями регуляторних пісочниць ШІ повинно бути сприяння інноваціям у сфері ШІ шляхом створення контрольованого середовища для експериментів та тестування на стадії розробки та передпродажної підготовки з метою забезпечення відповідності інноваційних систем ШІ цьому Регламенту та іншому відповідному законодавству Союзу та національному законодавству. Крім того, регуляторні пісочниці ШІ повинні прагнути підвищити правову визначеність для новаторів та нагляд

компетентних органів і розуміння ними можливостей, нових ризиків та наслідків використання ШІ, сприяти регуляторному навчанню для органів влади та підприємств, у тому числі з метою майбутньої адаптації правової бази, підтримувати співпрацю та обмін найкращими практиками з органами, залученими до регуляторної пісочниці ШІ, та прискорювати доступ до ринків, зокрема шляхом усунення бар'єрів для МСП, включаючи стартапи. Регуляторні пісочниці ШІ повинні бути широко доступними по всьому Союзу, і особливу увагу слід приділити їх доступності для МСП, включаючи стартапи. Участь у регуляторній пісочниці ШІ повинна зосереджуватися на питаннях, що породжують правову невизначеність для постачальників та перспективних постачальників щодо інновацій, експериментів із ШІ в Союзі та внеску в засноване на доказах регуляторне навчання. Тому нагляд за системами ШІ в регуляторній пісочниці ШІ має охоплювати їх розробку, навчання, тестування та валідацію до розміщення систем на ринку або введення їх в експлуатацію, а також поняття та випадки суттєвої модифікації, яка може вимагати нової процедури оцінки відповідності. Будь-які значні ризики, виявлені в ході розробки та тестування таких систем ШІ, повинні призводити до належного пом'якшення, а за його неможливості — до призупинення процесу розробки та тестування. Там, де це доречно, національні компетентні органи, що створюють регуляторні пісочниці ШІ, повинні співпрацювати з іншими відповідними органами, включаючи ті, що здійснюють нагляд за захистом основних прав, та можуть допускати залучення інших учасників екосистеми ШІ, як-от національні або європейські організації зі стандартизації, нотифіковані органи, об'єкти тестування та експериментів, дослідницькі та експериментальні лабораторії, Європейські цифрові інноваційні хаби та відповідні організації зацікавлених сторін і громадянського суспільства. Для забезпечення однакового виконання по всьому Союзу та досягнення економії від масштабу доречно встановити спільні правила для реалізації регуляторних пісочниць ШІ та систему співпраці

між відповідними органами, залученими до нагляду за пісочницями. Регуляторні пісочниці ШІ, створені відповідно до цього Регламенту, повинні бути без шкоди для іншого законодавства, що дозволяє створення інших пісочниць, спрямованих на забезпечення відповідності законодавству, відмінному від цього Регламенту. Там, де це доречно, відповідні компетентні органи, відповідальні за ці інші регуляторні пісочниці, повинні розглядати переваги використання таких пісочниць також з метою забезпечення відповідності систем ШІ цьому Регламенту. За згодою між національними компетентними органами та учасниками регуляторної пісочниці ШІ тестування в реальних умовах також може здійснюватися та контролюватися в рамках регуляторної пісочниці ШІ.

(140) Цей Регламент має забезпечити правову основу для постачальників та перспективних постачальників у регуляторній пісочниці ШІ щодо використання персональних даних, зібраних для інших цілей, для розробки певних систем ШІ в суспільних інтересах в рамках регуляторної пісочниці ШІ лише за визначених умов, відповідно до статті 6(4) та статті 9(2), пункт (g), Регламенту (ЄС) 2016/679, та статей 5, 6 і 10 Регламенту (ЄС) 2018/1725 та без шкоди для статті 4(2) та статті 10 Директиви (ЄС) 2016/680. Всі інші зобов'язання контролерів даних та права суб'єктів даних за Регламентами (ЄС) 2016/679 та (ЄС) 2018/1725 та Директивою (ЄС) 2016/680 залишаються застосовними. Зокрема, цей Регламент не повинен забезпечувати правову основу у значенні статті 22(2), пункт (b) Регламенту (ЄС) 2016/679 та статті 24(2), пункт (b) Регламенту (ЄС) 2018/1725. Постачальники та перспективні постачальники в регуляторній пісочниці ШІ повинні забезпечувати відповідні гарантії та співпрацювати з компетентними органами, включаючи дотримання їхніх вказівок та оперативні та сумлінні дії для належного пом'якшення будь-яких виявлених значних ризиків для безпеки, здоров'я та основних прав, що можуть виникнути в ході розробки, тестування та експериментів у такій пісочниці.

(141)

З метою прискорення процесу розробки та розміщення на ринку високоризикованих систем ШІ, перелічених у додатку до цього Регламенту, важливо, щоб постачальники або перспективні постачальники таких систем також могли скористатися спеціальним режимом тестування таких систем у реальних умовах без участі в регуляторній пісочниці ШІ. Однак у таких випадках, з урахуванням можливих наслідків такого тестування для осіб, слід забезпечити, щоб цим Регламентом для постачальників або перспективних постачальників були введені відповідні та достатні гарантії та умови. Такі гарантії повинні включати, зокрема, отримання інформованої згоди фізичних осіб на участь у тестуванні в реальних умовах, за винятком правоохоронної діяльності, де отримання інформованої згоди перешкоджало б тестуванню системи ШІ. Згода суб'єктів на участь у такому тестуванні відповідно до цього Регламенту є окремою від згоди суб'єктів даних на обробку їхніх персональних даних відповідно до відповідного законодавства про захист даних та не завдає їй шкоди. Також важливо мінімізувати ризики та забезпечити нагляд компетентних органів, і тому вимагати від перспективних постачальників подання плану тестування в реальних умовах до компетентного органу ринкового нагляду, реєстрації тестування у спеціальних розділах бази даних ЄС з урахуванням деяких обмежених винятків, встановлення обмежень на період, протягом якого може проводитися тестування, та вимагати додаткових гарантій для осіб, що належать до певних вразливих груп, а також письмової угоди, що визначає ролі та обов'язки перспективних постачальників та суб'єктів розгортання, та ефективного нагляду з боку компетентного персоналу, залученого до тестування в реальних умовах. Крім того, доречно передбачити додаткові гарантії для забезпечення того, щоб прогнози, рекомендації або рішення системи ШІ могли бути ефективно скасовані та проігноровані, а персональні дані захищені та видалені, коли суб'єкти відкликали свою згоду на участь у тестуванні без шкоди для їхніх прав як суб'єктів даних відповідно до законодавства Союзу про захист даних. Щодо передачі даних,

також доречно передбачити, що дані, зібрані та оброблені з метою тестування в реальних умовах, повинні передаватися в треті країни лише там, де впроваджено відповідні та застосовні гарантії відповідно до законодавства Союзу, зокрема відповідно до підстав для передачі персональних даних відповідно до законодавства Союзу про захист даних, тоді як для неперсональних даних впроваджуються відповідні гарантії відповідно до законодавства Союзу, наприклад Регламентів (ЄС) 2022/868 (42) та (ЄС) 2023/2854 (43) Європейського Парламенту і Ради.

(142) Для забезпечення того, щоб ШІ призводив до соціально та екологічно корисних результатів, держави-члени заохочуються підтримувати та просувати дослідження та розробку рішень ШІ на підтримку соціально та екологічно корисних результатів, таких як рішення на основі ШІ для підвищення доступності для осіб з інвалідністю, вирішення соціально-економічної нерівності або досягнення екологічних цілей, шляхом виділення достатніх ресурсів, включаючи державне фінансування та фінансування Союзу, та там, де це доречно та за умови виконання критеріїв прийнятності та відбору, розглядаючи зокрема проекти, що переслідують такі цілі. Такі проекти мають ґрунтуватися на принципі міждисциплінарної співпраці між розробниками ШІ, експертами з питань нерівності та недискримінації, доступності, правами споживачів, екологічними та цифровими правами, а також науковцями.

(143) З метою сприяння та захисту інновацій важливо, щоб інтереси МСП, включаючи стартапи, що є постачальниками або суб'єктами розгортання систем ШІ, враховувалися особливим чином. Для цього держави-члени повинні розробляти ініціативи, спрямовані на цих операторів, зокрема щодо підвищення обізнаності та інформаційного поширення. Держави-члени повинні надавати МСП, включаючи стартапи, що мають зареєстрований офіс або філію в Союзі, пріоритетний доступ до регуляторних пісочниць ШІ за умови виконання ними критеріїв прийнятності та відбору та без обмеження доступу інших постачальників та перспективних

постачальників до пісочниць за умови виконання тих самих умов та критеріїв. Держави-члени повинні використовувати існуючі канали та там, де це доречно, створювати нові спеціальні канали зв'язку з МСП, включаючи стартапи, суб'єктів розгортання, інших новаторів та, де це доречно, місцеві органи публічної влади для підтримки МСП протягом усього їхнього шляху розвитку шляхом надання вказівок та відповідей на запити щодо виконання цього Регламенту. Там, де це доречно, ці канали повинні співпрацювати для створення синергії та забезпечення однорідності у своїх вказівках МСП, включаючи стартапи, та суб'єктам розгортання. Крім того, держави-члени повинні сприяти участі МСП та інших відповідних зацікавлених сторін у процесах розробки стандартизації. Більше того, конкретні інтереси та потреби постачальників, що є МСП, включаючи стартапи, повинні враховуватися нотифікованими органами при встановленні плати за оцінку відповідності. Комісія повинна регулярно оцінювати витрати на сертифікацію та відповідність для МСП, включаючи стартапи, через прозорі консультації та повинна працювати з державами-членами для зниження таких витрат. Наприклад, витрати на переклад, пов'язані з обов'язковою документацією та спілкуванням з органами влади, можуть становити значні витрати для постачальників та інших операторів, зокрема тих, що мають менший масштаб. Держави-члени можливо повинні забезпечити, щоб однією з мов, визначених та прийнятих ними для документації відповідних постачальників та для спілкування з операторами, була мова, широко зрозуміла якомога більшій кількості транскордонних суб'єктів розгортання. З метою вирішення особливих потреб МСП, включаючи стартапи, Комісія повинна надавати стандартизовані шаблони для сфер, охоплених цим Регламентом, на запит Ради. Крім того, Комісія повинна доповнювати зусилля держав-членів шляхом надання єдиної інформаційної платформи з зручною для використання інформацією щодо цього Регламенту для всіх постачальників та суб'єктів розгортання, організації відповідних комунікаційних кампаній для підвищення обізнаності про зобов'язання, що випливають з

цього Регламенту, та оцінки та сприяння зближенню найкращих практик у процедурах публічних закупівель щодо систем ШІ. Підприємства середнього розміру, які до недавнього часу кваліфікувалися як малі підприємства у значенні Додатка до Рекомендації Комісії 2003/361/ЄС (44) повинні мати доступ до цих заходів підтримки, оскільки цим новим підприємствам середнього розміру може іноді бракувати правових ресурсів та навчання, необхідних для забезпечення належного розуміння та дотримання вимог цього Регламенту.

(144) З метою сприяння та захисту інновацій платформа ШІ на вимогу, всі відповідні програми та проекти фінансування Союзу, такі як програма «Цифрова Європа», «Горизонт Європа», що реалізуються Комісією та державами-членами на рівні Союзу або національному рівні, повинні, де це доречно, сприяти досягненню цілей цього Регламенту.

(145) З метою мінімізації ризиків для реалізації, що виникають внаслідок браку знань та досвіду на ринку, а також для полегшення виконання постачальниками, зокрема МСП, включаючи стартапи, та нотифікованими органами своїх зобов'язань відповідно до цього Регламенту, платформа ШІ на вимогу, Європейські цифрові інноваційні хаби та об'єкти тестування та експериментів, створені Комісією та державами-членами на рівні Союзу або національному рівні, повинні сприяти реалізації цього Регламенту. В межах своїх відповідних місій та сфер компетенції платформа ШІ на вимогу, Європейські цифрові інноваційні хаби та об'єкти тестування та експериментів здатні надавати, зокрема, технічну та наукову підтримку постачальникам та нотифікованим органам.

(146) Крім того, з огляду на дуже малий розмір деяких операторів та з метою забезпечення пропорційності щодо витрат на інновації доречно дозволити мікропідприємствам виконувати одне з найбільш затратних зобов'язань, а саме створення системи управління якістю, у спрощений спосіб, який зменшить адміністративне навантаження та витрати для

таких підприємств без впливу на рівень захисту та необхідність відповідності вимогам для високоризикованих систем ШІ. Комісія повинна розробити керівні настанови для визначення елементів системи управління якістю, які мають виконуватися мікропідприємствами у такий спрощений спосіб.

(147) Доречно, щоб Комісія сприяла, наскільки це можливо, доступу до об'єктів тестування та експериментів органам, групам або лабораторіям, створеним або акредитованим відповідно до будь-якого відповідного гармонізаційного законодавства Союзу та які виконують завдання в контексті оцінки відповідності продуктів або пристроїв, охоплених таким гармонізаційним законодавством Союзу. Це стосується, зокрема, експертних панелей, експертних лабораторій та референс-лабораторій у сфері медичних виробів відповідно до Регламентів (ЄС) 2017/745 та (ЄС) 2017/746.

(148) Цей Регламент має встановити систему управління, яка дозволяє як координувати та підтримувати застосування цього Регламенту на національному рівні, так і розвивати потенціал на рівні Союзу та залучати зацікавлені сторони у сфері ШІ. Ефективна реалізація та виконання цього Регламенту вимагають системи управління, яка дозволяє координувати та нарощувати центральну експертизу на рівні Союзу. Офіс ШІ було засновано Рішенням Комісії (45) та має своєю місією розвивати експертизу та потенціал Союзу в сфері ШІ та сприяти реалізації законодавства Союзу щодо ШІ. Держави-члени повинні сприяти виконанню завдань Офісу ШІ з метою підтримки розвитку експертизи та потенціалу Союзу на рівні Союзу та зміцнення функціонування єдиного цифрового ринку. Крім того, має бути створено Раду у складі представників держав-членів, наукову панель для залучення наукової спільноти та дорадчий форум для внеску зацікавлених сторін у реалізацію цього Регламенту на рівні Союзу та національному рівні. Розвиток експертизи та потенціалу Союзу повинен також включати використання існуючих ресурсів та досвіду, зокрема через синергію зі структурами,

створеними в контексті виконання іншого законодавства на рівні Союзу, та синергію з відповідними ініціативами на рівні Союзу, такими як Спільне підприємство EuroHPC та об'єкти тестування та експериментів ШІ в рамках програми «Цифрова Європа».

(149) З метою сприяння плавному, ефективному та гармонізованому виконанню цього Регламенту слід створити Раду. Рада повинна відображати різноманітні інтереси екосистеми ШІ та складатися з представників держав-членів. Рада несе відповідальність за низку консультативних завдань, включаючи видачу висновків, рекомендацій, порад або участь у розробці вказівок з питань, пов'язаних із виконанням цього Регламенту, зокрема з питань примусового виконання, технічних специфікацій або існуючих стандартів щодо вимог, встановлених у цьому Регламенті, та надання порад Комісії та державам-членам та їхнім національним компетентним органам з конкретних питань, пов'язаних із ШІ. З метою надання певної гнучкості державам-членам при призначенні своїх представників у Раді такі представники можуть бути будь-якими особами, що належать до публічних органів, які повинні мати відповідні компетенції та повноваження для полегшення координації на національному рівні та сприяння досягненню завдань Ради. Рада повинна створити дві постійні підгрупи для забезпечення платформи для співпраці та обміну між органами ринкового нагляду та нотифікуючими органами з питань, що стосуються відповідно ринкового нагляду та нотифікованих органів. Постійна підгрупа з ринкового нагляду повинна виступати як адміністративна група зі співробітництва (ADCO) для цього Регламенту у значенні статті 30 Регламенту (ЄС) 2019/1020. Відповідно до статті 33 зазначеного Регламенту Комісія повинна підтримувати діяльність постійної підгрупи з ринкового нагляду шляхом проведення ринкових оцінок або досліджень, зокрема з метою визначення аспектів цього Регламенту, що потребують конкретної та невідкладної координації між органами ринкового нагляду. Рада може за необхідності створювати інші постійні або тимчасові підгрупи для вивчення

конкретних питань. Рада також повинна співпрацювати, де це доречно, з відповідними органами Союзу, групами експертів та мережами, що діють у контексті відповідного законодавства Союзу, зокрема тими, що діють відповідно до відповідного законодавства Союзу щодо даних, цифрових продуктів та послуг.

(150) З метою забезпечення залучення зацікавлених сторін до виконання та застосування цього Регламенту слід створити дорадчий форум для консультування та надання технічної експертизи Раді та Комісії. Для забезпечення різноманітного та збалансованого представництва зацікавлених сторін між комерційними та некомерційними інтересами та в категорії комерційних інтересів щодо МСП та інших підприємств дорадчий форум повинен включати, зокрема, промисловість, стартапи, МСП, академічну спільноту, громадянське суспільство, включаючи соціальних партнерів, а також Агентство основних прав, ENISA, Європейський комітет зі стандартизації (CEN), Європейський комітет з електротехнічної стандартизації (CENELEC) та Європейський інститут телекомунікаційних стандартів (ETSI).

(151) Для підтримки реалізації та виконання цього Регламенту, зокрема моніторингової діяльності Офісу ШІ щодо загальноцільових моделей ШІ, слід створити наукову панель незалежних експертів. Незалежні експерти, що складають наукову панель, повинні відбиратися на основі актуальних наукових або технічних знань у сфері ШІ та виконувати свої завдання неупереджено, об'єктивно та забезпечувати конфіденційність інформації та даних, отриманих при виконанні їхніх завдань і діяльності. Для зміцнення національного потенціалу, необхідного для ефективного виконання цього Регламенту, держави-члени повинні мати можливість запитувати підтримку від пулу експертів, що складають наукову панель, для їхніх заходів виконання.

(152) З метою підтримки належного виконання щодо систем ШІ та зміцнення потенціалу держав-членів слід створити структури підтримки

тестування ШІ Союзу та зробити їх доступними для держав-членів.

(153) Держави-члени відіграють ключову роль у застосуванні та виконанні цього Регламенту. У цьому відношенні кожна держава-член повинна призначити принаймні один нотифікуючий орган та принаймні один орган ринкового нагляду як національні компетентні органи з метою нагляду за застосуванням та виконанням цього Регламенту. Держави-члени можуть вирішити призначити будь-який вид публічного органу для виконання завдань національних компетентних органів у значенні цього Регламенту відповідно до їхніх конкретних національних організаційних особливостей та потреб. З метою підвищення організаційної ефективності держав-членів та встановлення єдиної точки контакту щодо громадськості та інших контрагентів на рівні держав-членів та Союзу кожна держава-член повинна призначити орган ринкового нагляду для виконання функцій єдиної точки контакту.

(154) Національні компетентні органи повинні здійснювати свої повноваження незалежно, неупереджено та без упередженості з метою захисту принципів об'єктивності їхньої діяльності та завдань і забезпечення застосування та виконання цього Регламенту. Члени цих органів повинні утримуватися від будь-яких дій, несумісних з їхніми обов'язками, та повинні підпадати під правила конфіденційності відповідно до цього Регламенту.

(155) З метою забезпечення того, щоб постачальники високоризикованих систем ШІ могли враховувати досвід використання таких систем для вдосконалення своїх систем та процесу проектування і розробки або могли своєчасно вживати будь-яких можливих коригувальних заходів, усі постачальники повинні мати систему постринкового моніторингу. Де це актуально, постринковий моніторинг повинен включати аналіз взаємодії з іншими системами ШІ, включаючи інші пристрої та програмне забезпечення. Постринковий моніторинг не повинен охоплювати чутливі оперативні дані суб'єктів розгортання, які є правоохоронними

органами. Ця система також є ключовою для забезпечення того, щоб можливі ризики, що виникають з систем ШІ, які продовжують «навчатися» після розміщення на ринку або введення в експлуатацію, могли бути вирішені більш ефективно та своєчасно. У цьому контексті постачальники також повинні бути зобов'язані мати систему для повідомлення відповідних органів про будь-які серйозні інциденти, що виникли внаслідок використання їхніх систем ШІ, тобто інциденти або несправності, що призводять до смерті або серйозної шкоди здоров'ю, серйозних та незворотних порушень управління та функціонування критичної інфраструктури, порушень зобов'язань відповідно до законодавства Союзу, спрямованих на захист основних прав, або серйозної шкоди майну або навколишньому середовищу.

(156) З метою забезпечення належного та ефективного виконання вимог та зобов'язань, встановлених цим Регламентом, що є гармонізаційним законодавством Союзу, система ринкового нагляду та відповідності продуктів, встановлена Регламентом (ЄС) 2019/1020, повинна застосовуватися в повному обсязі. Органи ринкового нагляду, призначені відповідно до цього Регламенту, повинні мати всі повноваження у сфері примусового виконання, передбачені цим Регламентом та Регламентом (ЄС) 2019/1020, та повинні здійснювати свої повноваження та виконувати свої обов'язки незалежно, неупереджено та без упередженості. Хоча більшість систем ШІ не підлягає конкретним вимогам та зобов'язанням відповідно до цього Регламенту, органи ринкового нагляду можуть вживати заходів щодо всіх систем ШІ, коли вони становлять ризик відповідно до цього Регламенту. З огляду на специфічну природу установ, агентств та органів Союзу, що підпадають під сферу застосування цього Регламенту, доречно призначити Європейського наглядача із захисту даних компетентним органом ринкового нагляду для них. Це має бути без шкоди для призначення національних компетентних органів державами-членами. Діяльність з ринкового нагляду не повинна впливати на здатність піднаглядних

суб'єктів виконувати свої завдання незалежно, коли така незалежність вимагається законодавством Союзу.

(157) Цей Регламент не завдає шкоди компетенціям, завданням, повноваженням та незалежності відповідних національних публічних органів або органів влади, які здійснюють нагляд за застосуванням законодавства Союзу щодо захисту основних прав, включаючи органи із забезпечення рівності та органи захисту даних. Там, де це необхідно для їхнього мандату, ці національні публічні органи або органи влади повинні також мати доступ до будь-якої документації, створеної відповідно до цього Регламенту. Слід встановити спеціальну захисну процедуру для забезпечення належного та своєчасного виконання щодо систем ШІ, що становлять ризик для здоров'я, безпеки та основних прав. Процедура для таких систем ШІ, що становлять ризик, має застосовуватися до високоризикованих систем ШІ, що становлять ризик, заборонених систем, що були розміщені на ринку, введені в експлуатацію або використані в порушення заборонених практик, встановлених цим Регламентом, та систем ШІ, що були зроблені доступними в порушення вимог прозорості, встановлених цим Регламентом, і становлять ризик.

(158) Законодавство Союзу про фінансові послуги включає правила та вимоги щодо внутрішнього управління та управління ризиками, що застосовуються до регульованих фінансових установ у процесі надання таких послуг, зокрема коли вони використовують системи ШІ. З метою забезпечення послідовного застосування та виконання зобов'язань за цим Регламентом та відповідних правил та вимог правових актів Союзу про фінансові послуги компетентні органи для нагляду та виконання таких правових актів, зокрема компетентні органи, як це визначено в Регламенті (ЄС) № 575/2013 Європейського Парламенту і Ради (46) та Директивах 2008/48/ЄС (47), 2009/138/ЄС (48), 2013/36/ЄС (49), 2014/17/ЄС (50) та (ЄС) 2016/97 (51) Європейського Парламенту і Ради мають бути призначені в межах своїх відповідних

компетенцій як компетентні органи з метою нагляду за виконанням цього Регламенту, включаючи для заходів ринкового нагляду, щодо систем ШІ, що надаються або використовуються регульованими та піднаглядними фінансовими установами, якщо держави-члени не вирішать призначити інший орган для виконання цих завдань ринкового нагляду. Ці компетентні органи повинні мати всі повноваження відповідно до цього Регламенту та Регламенту (ЄС) 2019/1020 для забезпечення виконання вимог та зобов'язань цього Регламенту, включаючи повноваження для проведення ex post заходів ринкового нагляду, які можуть бути інтегровані, де це доречно, до їхніх існуючих наглядових механізмів та процедур відповідно до відповідного законодавства Союзу про фінансові послуги. Доречно передбачити, що при виконанні функцій органів ринкового нагляду відповідно до цього Регламенту національні органи, відповідальні за нагляд за кредитними установами, що регулюються Директивою 2013/36/ЄС та беруть участь у Єдиному наглядовому механізмі, створеному Регламентом Ради (ЄС) № 1024/2013 (52), повинні без затримки повідомляти Європейський центральний банк про будь-яку інформацію, виявлену в ході їхньої діяльності з ринкового нагляду, яка може представляти потенційний інтерес для пруденційних наглядових завдань Європейського центрального банку, як це визначено в зазначеному Регламенті. Для подальшого підвищення узгодженості між цим Регламентом та правилами, застосовними до кредитних установ, що регулюються Директивою 2013/36/ЄС, також доречно інтегрувати деякі процедурні зобов'язання постачальників щодо управління ризиками, постринкового моніторингу та документації до існуючих зобов'язань та процедур відповідно до Директиви 2013/36/ЄС. З метою уникнення дублювання слід також передбачити обмежені відступи стосовно системи управління якістю постачальників та зобов'язання щодо моніторингу, покладеного на суб'єктів розгортання високоризикованих систем ШІ, тією мірою, якою вони застосовуються до кредитних установ, що регулюються Директивою 2013/36/ЄС. Той самий режим має

застосовуватися до страхових та перестрахових компаній і страхових холдингових компаній відповідно до Директиви 2009/138/ЄС та страхових посередників відповідно до Директиви (ЄС) 2016/97 та інших видів фінансових установ, що підлягають вимогам щодо внутрішнього управління, заходів або процесів, встановлених відповідно до відповідного законодавства Союзу про фінансові послуги, для забезпечення послідовності та рівного ставлення у фінансовому секторі.

(159) Кожен орган ринкового нагляду за високоризикованими системами ШІ у сфері біометрії, перерахованими в додатку до цього Регламенту, тією мірою, якою такі системи використовуються для цілей правоохоронної діяльності, міграції, притулку та управління кордонами або відправлення правосуддя та демократичних процесів, повинен мати ефективні слідчі та коригувальні повноваження, включаючи принаймні повноваження отримувати доступ до всіх персональних даних, що обробляються, та до всієї інформації, необхідної для виконання його завдань. Органи ринкового нагляду повинні мати можливість здійснювати свої повноваження, діючи з повною незалежністю. Будь-які обмеження їхнього доступу до чутливих оперативних даних відповідно до цього Регламенту мають бути без шкоди для повноважень, наданих їм Директивою (ЄС) 2016/680. Жодне виключення щодо розкриття даних національним органам захисту даних відповідно до цього Регламенту не повинно впливати на поточні або майбутні повноваження цих органів поза межами сфери застосування цього Регламенту.

(160) Органи ринкового нагляду та Комісія повинні мати можливість пропонувати спільні заходи, включаючи спільні розслідування, що проводяться органами ринкового нагляду або органами ринкового нагляду спільно з Комісією, спрямовані на сприяння відповідності, виявлення невідповідності, підвищення обізнаності та надання вказівок щодо цього Регламенту стосовно конкретних категорій високоризикованих систем ШІ, які, як виявлено,

становлять серйозний ризик у двох або більше державах-членах. Спільні заходи з просування відповідності мають здійснюватися відповідно до статті 9 Регламенту (ЄС) 2019/1020. Офіс ШІ повинен надавати координаційну підтримку для спільних розслідувань.

(161) Необхідно уточнити відповідальність та компетенції на рівні Союзу та національному рівні щодо систем ШІ, що побудовані на загальноцільових моделях ШІ. Для уникнення дублювання компетенцій, якщо система ШІ ґрунтується на загальноцільовій моделі ШІ та модель і система надаються одним і тим самим постачальником, нагляд повинен здійснюватися на рівні Союзу через Офіс ШІ, який повинен мати повноваження органу ринкового нагляду у значенні Регламенту (ЄС) 2019/1020 для цієї мети. У всіх інших випадках національні органи ринкового нагляду залишаються відповідальними за нагляд за системами ШІ. Однак для загальноцільових систем ШІ, які можуть використовуватися суб'єктами розгортання безпосередньо принаймні для однієї мети, що класифікується як високоризикована, органи ринкового нагляду повинні співпрацювати з Офісом ШІ для проведення оцінок відповідності та відповідного інформування Ради та інших органів ринкового нагляду. Крім того, органи ринкового нагляду повинні мати можливість звертатися за допомогою до Офісу ШІ у випадках, коли орган ринкового нагляду не може завершити розслідування щодо високоризикованої системи ШІ через неможливість доступу до певної інформації, пов'язаної із загальноцільовою моделлю ШІ, на якій побудована ця система. У таких випадках має застосовуватися процедура взаємної допомоги у транскордонних справах відповідно до Глави VI Регламенту (ЄС) 2019/1020 mutatis mutandis.

(162) Для найкращого використання централізованої експертизи Союзу та синергій на рівні Союзу повноваження нагляду та виконання зобов'язань постачальників загальноцільових моделей ШІ мають бути компетенцією Комісії. Офіс ШІ повинен мати можливість вживати всіх

необхідних заходів для моніторингу ефективної реалізації цього Регламенту щодо загальноцільових моделей ШІ. Він повинен мати можливість розслідувати можливі порушення правил щодо постачальників загальноцільових моделей ШІ як за власною ініціативою, за результатами своєї моніторингової діяльності, так і на запит органів ринкового нагляду відповідно до умов, встановлених цим Регламентом. Для підтримки ефективного моніторингу Офісу ШІ слід передбачити можливість для постачальників нижньої ланки подавати скарги щодо можливих порушень правил стосовно постачальників загальноцільових моделей та систем ШІ.

(163) З метою доповнення систем управління загальноцільовими моделями ШІ наукова панель повинна підтримувати моніторингову діяльність Офісу ШІ та може в певних випадках надавати кваліфіковані попередження Офісу ШІ, які ініціюють подальші дії, такі як розслідування. Це має бути у випадках, коли наукова панель має підстави підозрювати, що загальноцільова модель ШІ становить конкретний та ідентифікований ризик на рівні Союзу. Крім того, це має бути у випадках, коли наукова панель має підстави підозрювати, що загальноцільова модель ШІ відповідає критеріям, що призведуть до її класифікації як загальноцільової моделі ШІ із системним ризиком. Для оснащення наукової панелі інформацією, необхідною для виконання цих завдань, має бути механізм, за допомогою якого наукова панель може просити Комісію вимагати документацію або інформацію від постачальника.

(164) Офіс ШІ повинен мати можливість вживати необхідних заходів для моніторингу ефективної реалізації та дотримання зобов'язань для постачальників загальноцільових моделей ШІ, встановлених цим Регламентом. Офіс ШІ повинен мати можливість розслідувати можливі порушення відповідно до повноважень, передбачених цим Регламентом, зокрема шляхом запиту документації та інформації, проведення оцінок, а також запиту заходів від постачальників загальноцільових моделей ШІ. При проведенні

оцінок, з метою використання незалежної експертизи, Офіс ШІ повинен мати можливість залучати незалежних експертів для проведення оцінок від свого імені. Виконання зобов'язань має бути забезпечуваним примусово, зокрема через запити про вжиття відповідних заходів, включаючи заходи із зменшення ризиків у випадку виявлених системних ризиків, а також обмеження надання на ринку, вилучення або відкликання моделі. Як гарантія, де це необхідно понад процедурні права, передбачені цим Регламентом, постачальники загальноцільових моделей ШІ повинні мати процедурні права, передбачені статтею 18 Регламенту (ЄС) 2019/1020, що має застосовуватися mutatis mutandis, без шкоди для більш конкретних процедурних прав, передбачених цим Регламентом.

(165) Розробка систем ШІ, відмінних від високоризикованих, відповідно до вимог цього Регламенту може призвести до більш широкого впровадження етичного та надійного ШІ в Союзі. Постачальників систем ШІ, які не є високоризикованими, слід заохочувати до розробки кодексів поведінки, включаючи пов'язані механізми управління, спрямованих на сприяння добровільному застосуванню деяких або всіх обов'язкових вимог, застосовних до високоризикованих систем ШІ, адаптованих з урахуванням передбаченого призначення систем та меншого ризику, що виникає, та з урахуванням доступних технічних рішень та найкращих галузевих практик, таких як картки моделей та даних. Постачальників та, де це доречно, суб'єктів розгортання всіх систем ШІ, незалежно від того, чи є вони високоризикованими, та моделей ШІ також слід заохочувати до добровільного застосування додаткових вимог, пов'язаних, наприклад, з елементами Етичних принципів Союзу для надійного ШІ, екологічною стійкістю, заходами щодо освіченості у сфері ШІ, інклюзивним та різноманітним проектуванням та розробкою систем ШІ, включаючи увагу до вразливих осіб та доступності для осіб з інвалідністю, участю зацікавлених сторін із залученням, де це доречно, відповідних зацікавлених сторін, таких

як підприємства та організації громадянського суспільства, академічна спільнота, дослідницькі організації, профспілки та організації захисту споживачів у проектуванні та розробці систем ШІ, та різноманітністю команд розробки, включаючи гендерний баланс. Для забезпечення ефективності добровільних кодексів поведінки вони повинні ґрунтуватися на чітких цілях та ключових показниках ефективності для вимірювання досягнення цих цілей. Вони також мають розроблятися інклюзивним способом, де це доречно, із залученням відповідних зацікавлених сторін, таких як підприємства та організації громадянського суспільства, академічна спільнота, дослідницькі організації, профспілки та організації захисту споживачів. Комісія може розробляти ініціативи, включаючи галузеві, для сприяння зниженню технічних бар'єрів, що перешкоджають транскордонному обміну даними для розвитку ШІ, включаючи інфраструктуру доступу до даних, семантичну та технічну сумісність різних типів даних.

(166) Важливо, щоб системи ШІ, пов'язані з продуктами, які не є високоризикованими відповідно до цього Регламенту та тому не зобов'язані відповідати вимогам, встановленим для високоризикованих систем ШІ, були, тим не менш, безпечними при розміщенні на ринку або введенні в експлуатацію. Для сприяння досягненню цієї мети застосовуватиметься Регламент (ЄС) 2023/988 Європейського Парламенту і Ради (53) як захисна мережа.

(167) З метою забезпечення довірчої та конструктивної співпраці компетентних органів на рівні Союзу та національному рівні всі сторони, залучені до застосування цього Регламенту, повинні дотримуватися конфіденційності інформації та даних, отриманих при виконанні їхніх завдань, відповідно до законодавства Союзу або національного законодавства. Вони повинні виконувати свої завдання та здійснювати свою діяльність таким чином, щоб захищати, зокрема, права інтелектуальної власності, конфіденційну ділову інформацію та комерційні таємниці, ефективне виконання цього Регламенту, інтереси

суспільної та національної безпеки, цілісність кримінальних та адміністративних проваджень, а також цілісність секретної інформації.

(168) Дотримання цього Регламенту повинно забезпечуватися примусово шляхом накладення санкцій та інших заходів виконання. Держави-члени повинні вживати всіх необхідних заходів для забезпечення реалізації положень цього Регламенту, включаючи встановлення ефективних, пропорційних та таких, що стримують, санкцій за їх порушення, та дотримання принципу ne bis in idem . З метою зміцнення та гармонізації адміністративних санкцій за порушення цього Регламенту слід встановити верхні межі для встановлення адміністративних штрафів за певні конкретні порушення. При оцінці розміру штрафів держави-члени повинні в кожному окремому випадку враховувати всі відповідні обставини конкретної ситуації, з належним урахуванням, зокрема, характеру, тяжкості та тривалості порушення та його наслідків, а також розміру постачальника, зокрема якщо постачальник є МСП, включаючи стартап. Європейський наглядач із захисту даних повинен мати повноваження накладати штрафи на установи, агентства та органи Союзу, що підпадають під сферу застосування цього Регламенту.

(169) Виконання зобов'язань постачальників загальноцільових моделей ШІ, встановлених відповідно до цього Регламенту, має забезпечуватися примусово, зокрема, шляхом накладення штрафів. Для цього також слід встановити відповідні рівні штрафів за порушення цих зобов'язань, включаючи невиконання заходів, запрошених Комісією відповідно до цього Регламенту, з урахуванням відповідних строків позовної давності відповідно до принципу пропорційності. Всі рішення, ухвалені Комісією відповідно до цього Регламенту, підлягають перегляду Судом справедливості Європейського Союзу відповідно до ДФЄС, включаючи необмежену юрисдикцію Суду справедливості щодо санкцій відповідно до статті 261 ДФЄС.

(170) Законодавство Союзу та національне законодавство вже передбачають ефективні засоби правового захисту для фізичних та юридичних осіб, права та свободи яких негативно зачіпаються внаслідок використання систем ШІ. Без шкоди для цих засобів захисту будь-яка фізична або юридична особа, яка має підстави вважати, що мало місце порушення цього Регламенту, повинна мати право подати скаргу до відповідного органу ринкового нагляду.

(171) Постраждалі особи повинні мати право на отримання пояснення у випадках, коли рішення суб'єкта розгортання базується головним чином на вихідних даних певних високоризикованих систем ШІ, що підпадають під сферу застосування цього Регламенту, і це рішення породжує правові наслідки або подібним чином суттєво впливає на цих осіб таким чином, що вони вважають таким, що має несприятливий вплив на їхнє здоров'я, безпеку або основні права. Таке пояснення має бути чітким та значущим і має надавати основу, на якій постраждалі особи здатні здійснювати свої права. Право на отримання пояснення не повинно застосовуватися до використання систем ШІ, для яких з законодавства Союзу або національного законодавства випливають виключення або обмеження, та повинно застосовуватися лише тою мірою, якою це право ще не передбачено законодавством Союзу.

(172) Особи, які повідомляють про порушення цього Регламенту як викривачі, повинні бути захищені відповідно до законодавства Союзу. Директива (ЄС) 2019/1937 Європейського Парламенту і Ради (54) тому має застосовуватися до повідомлення про порушення цього Регламенту та захисту осіб, що повідомляють про такі порушення.

(173) З метою забезпечення можливості адаптації регуляторної бази там, де це необхідно, Комісії слід делегувати повноваження на прийняття актів відповідно до статті 290 ДФЄС для внесення змін до умов, за яких система ШІ не вважається високоризикованою, переліку високоризикованих систем ШІ, положень щодо технічної документації, змісту декларації

відповідності ЄС, положень щодо процедур оцінки відповідності, положень, що встановлюють високоризиковані системи ШІ, до яких має застосовуватися процедура оцінки відповідності на основі оцінки системи управління якістю та оцінки технічної документації, порогу, орієнтирів та показників, включаючи доповнення цих орієнтирів та показників, у правилах класифікації загальноцільових моделей ШІ із системним ризиком, критеріїв для визначення загальноцільових моделей ШІ із системним ризиком, технічної документації для постачальників загальноцільових моделей ШІ та інформації про прозорість для постачальників загальноцільових моделей ШІ. Особливо важливо, щоб Комісія проводила відповідні консультації в ході своїх підготовчих робіт, у тому числі на рівні експертів, і щоб ці консультації проводилися відповідно до принципів, встановлених Міжінституційною угодою від 13 квітня 2016 року про краще законотворення (55). Зокрема, для забезпечення рівної участі в підготовці делегованих актів Європейський Парламент та Рада отримують всі документи одночасно з експертами держав-членів, і їхні експерти систематично мають доступ до засідань груп експертів Комісії, що займаються підготовкою делегованих актів.

(174) З огляду на швидкий технологічний розвиток та технічну експертизу, необхідну для ефективного застосування цього Регламенту, Комісія повинна оцінювати та переглядати цей Регламент до 2 серпня 2029 року та кожні чотири роки після цього та звітувати перед Європейським Парламентом та Радою. Крім того, з урахуванням наслідків для сфери застосування цього Регламенту Комісія повинна проводити оцінку необхідності внесення змін до переліку високоризикованих систем ШІ та переліку заборонених практик раз на рік. Більше того, до 2 серпня 2028 року та кожні чотири роки після цього Комісія повинна оцінювати та звітувати перед Європейським Парламентом та Радою про необхідність внесення змін до переліку заголовків сфер високого ризику в додатку до цього Регламенту, систем ШІ в рамках

зобов'язань щодо прозорості, ефективності системи нагляду та управління та прогресу в розробці результатів стандартизації щодо енергоефективної розробки загальноцільових моделей ШІ, включаючи необхідність подальших заходів або дій. Нарешті, до 2 серпня 2028 року та кожні три роки після цього Комісія повинна оцінювати вплив та ефективність добровільних кодексів поведінки для сприяння застосуванню вимог, передбачених для високоризикованих систем ШІ, у випадку систем ШІ, відмінних від високоризикованих, та, можливо, інших додаткових вимог для таких систем ШІ.

(175) З метою забезпечення однакових умов для реалізації цього Регламенту Комісії слід надати виконавчі повноваження. Ці повноваження повинні здійснюватися відповідно до Регламенту (ЄС) № 182/2011 Європейського Парламенту і Ради (56).

(176) Оскільки мета цього Регламенту, а саме вдосконалення функціонування внутрішнього ринку та сприяння поширенню людиноцентричного та надійного ШІ при забезпеченні високого рівня захисту здоров'я, безпеки, основних прав, закріплених у Хартії, включаючи демократію, верховенство права та захист навколишнього середовища від шкідливих наслідків систем ШІ в Союзі та підтримки інновацій, не може бути достатньою мірою досягнута державами-членами та натомість, з огляду на масштаб або наслідки дій, може бути краще досягнута на рівні Союзу, Союз може вживати заходів відповідно до принципу субсидіарності, передбаченого статтею 5 ДЄС. Відповідно до принципу пропорційності, передбаченого цією статтею, цей Регламент не виходить за межі того, що необхідно для досягнення цієї мети.

(177) З метою забезпечення правової визначеності, забезпечення відповідного адаптаційного періоду для операторів та уникнення збоїв на ринку, зокрема шляхом забезпечення безперервності використання систем ШІ, доречно, щоб цей Регламент застосовувався до високоризикованих систем ШІ, що були розміщені на ринку або введені в експлуатацію до загальної дати його

застосування, лише за умови, що з цієї дати такі системи зазнають значних змін у своєму проектуванні або передбаченому призначенні. Доречно уточнити, що в цьому відношенні поняття значної зміни слід розуміти як рівнозначне по суті поняттю суттєвої модифікації, яке використовується стосовно лише високоризикованих систем ШІ відповідно до цього Регламенту. В порядку виключення та з урахуванням публічної підзвітності оператори систем ШІ, що є компонентами великомасштабних ІТ-систем, створених правовими актами, переліченими в додатку до цього Регламенту, та оператори високоризикованих систем ШІ, призначених для використання органами публічної влади, повинні відповідно вжити необхідних кроків для виконання вимог цього Регламенту до кінця 2030 року та до 2 серпня 2030 року.

(178) Постачальників високоризикованих систем ШІ заохочують добровільно розпочати виконання відповідних зобов'язань цього Регламенту вже в перехідний період.

(179) Цей Регламент має застосовуватися з 2 серпня 2026 року. Однак, з урахуванням неприйнятного ризику, пов'язаного з використанням ШІ певними способами, заборони, а також загальні положення цього Регламенту повинні вже застосовуватися з 2 лютого 2025 року. Хоча повний ефект цих заборон настає зі встановленням системи управління та виконання цього Регламенту, передбачення застосування заборон є важливим для врахування неприйнятних ризиків та впливу на інші процедури, такі як цивільне право. Крім того, інфраструктура, пов'язана із системою управління та оцінки відповідності, має бути операційною до 2 серпня 2026 року, тому положення про нотифіковані органи та структуру управління мають застосовуватися з 2 серпня 2025 року. З огляду на швидкий темп технологічного прогресу та впровадження загальноцільових моделей ШІ зобов'язання для постачальників загальноцільових моделей ШІ мають застосовуватися з 2 серпня 2025 року. Кодекси практики мають бути готові до 2 травня

2025 року з метою надання постачальникам можливості своєчасно продемонструвати відповідність. Офіс ШІ повинен забезпечити актуальність правил та процедур класифікації з урахуванням технологічних розробок. Крім того, держави-члени повинні встановити та повідомити Комісії правила щодо санкцій, включаючи адміністративні штрафи, та забезпечити їх належне та ефективне застосування до дати застосування цього Регламенту. Тому положення про санкції мають застосовуватися з 2 серпня 2025 року.

(180) З Європейським наглядачем із захисту даних та Європейською радою із захисту даних були проведені консультації відповідно до статті 42(1) та (2) Регламенту (ЄС) 2018/1725, і вони надали свій спільний висновок 18 червня 2021 року,

HAVE ADOPTED THIS REGULATION:

ГЛАВА I

ЗАГАЛЬНІ ПОЛОЖЕННЯ

Стаття 1

Предмет регулювання

1. Метою цього Регламенту є вдосконалення функціонування внутрішнього ринку та сприяння поширенню людиноцентричного та надійного штучного інтелекту (ШІ) при забезпеченні високого рівня захисту здоров'я, безпеки, основних прав, закріплених у Хартії, включаючи демократію, верховенство права та захист навколишнього середовища, від шкідливих наслідків систем ШІ в Союзі та підтримки інновацій.

2. Цей Регламент встановлює:

(a) гармонізовані правила щодо розміщення на ринку, введення в експлуатацію та використання систем ШІ в Союзі;

(b) заборони певних практик ШІ;

(c) конкретні вимоги до високоризикованих систем ШІ та зобов'язання для операторів таких систем;

(d) гармонізовані правила прозорості для певних систем ШІ;

(e) гармонізовані правила щодо розміщення на ринку загальноцільових моделей ШІ;

(f) правила щодо моніторингу ринку, ринкового нагляду, управління та виконання;

(g) заходи для підтримки інновацій з особливим акцентом на МСП, включаючи стартапи.

Стаття 2

Сфера застосування

1. Цей Регламент застосовується до:

(a) постачальників, що розміщують на ринку або вводять в експлуатацію системи ШІ або розміщують на ринку загальноцільові моделі ШІ в Союзі, незалежно від того, чи засновані або розташовані такі постачальники в Союзі або в третій країні;

(b) суб'єктів розгортання систем ШІ, що мають місце реєстрації або розташовані в Союзі;

(c) постачальників та суб'єктів розгортання систем ШІ, що мають місце реєстрації або розташовані в третій країні, де вихідні дані, вироблені системою ШІ, використовуються в Союзі;

(d) імпортерів та дистриб'юторів систем ШІ;

(e) виробників продуктів, що розміщують на ринку або вводять в експлуатацію систему ШІ разом зі своїм продуктом та під власним іменем або торговельною маркою;

(f) уповноважених представників постачальників, не заснованих в Союзі;

(g) постраждалих осіб, що розташовані в Союзі.

2. Для систем ШІ, класифікованих як високоризикові відповідно до статті 6(1) стосовно продуктів, охоплених гармонізаційним законодавством Союзу, переліченим у розділі B Додатка I, застосовуються лише стаття 6(1), статті 102–109 та стаття 112. Стаття 57 застосовується лише тією мірою, якою вимоги до високоризикованих систем ШІ відповідно до цього Регламенту були інтегровані у таке гармонізаційне законодавство Союзу.

3. Цей Регламент не застосовується до сфер, що виходять за межі законодавства Союзу, та жодним чином не впливає на компетенції держав-членів щодо національної безпеки, незалежно від виду суб'єкта, якому доручено державами-членами виконання завдань у зв'язку з цими компетенціями.

Цей Регламент не застосовується до систем ШІ там і тією мірою, де та якою вони розміщуються на ринку, вводяться в експлуатацію або використовуються зі змінами або без змін виключно для військових, оборонних або цілей національної безпеки, незалежно від виду суб'єкта, що здійснює такі дії.

Цей Регламент не застосовується до систем ШІ, що не розміщуються на ринку або не вводяться в експлуатацію в Союзі, де вихідні дані використовуються в Союзі виключно для військових, оборонних або цілей національної безпеки, незалежно від виду суб'єкта, що здійснює такі дії.

4. Цей Регламент не застосовується ні до органів публічної влади третьої країни, ні до міжнародних організацій, що підпадають під сферу застосування цього Регламенту відповідно до пункту 1, де такі органи або організації використовують системи ШІ в рамках міжнародної співпраці або угод про правоохоронну та судову співпрацю з Союзом або з одною чи кількома державами-членами, за умови, що така третя країна або міжнародна організація надає достатні гарантії щодо захисту основних прав і свобод осіб.

5. Цей Регламент не впливає на застосування положень про відповідальність постачальників посередницьких послуг, викладених у Главі II Регламенту (ЄС) 2022/2065.

6. Цей Регламент не застосовується до систем ШІ або моделей ШІ, включаючи їхні вихідні дані, спеціально розроблених та введених в експлуатацію виключно з метою наукових досліджень та розробок.

7. Законодавство Союзу про захист персональних даних, приватність та конфіденційність комунікацій застосовується до персональних даних, що обробляються у зв'язку з правами та зобов'язаннями, встановленими в цьому Регламенті. Цей Регламент не впливає на Регламент (ЄС) 2016/679 або (ЄС) 2018/1725, або Директиву 2002/58/ЄС або (ЄС) 2016/680, без шкоди для статті 10(5) та статті 59 цього Регламенту.

8. Цей Регламент не застосовується до будь-яких досліджень, тестування або діяльності з розробки щодо систем ШІ або моделей ШІ до їх розміщення на ринку або введення в експлуатацію. Така діяльність здійснюється відповідно до застосовного законодавства Союзу. Тестування в реальних умовах не підпадає під це виключення.

9. Цей Регламент не завдає шкоди правилам, встановленим іншими правовими актами Союзу, пов'язаними із захистом споживачів та безпекою продуктів.

10. Цей Регламент не застосовується до зобов'язань суб'єктів розгортання, які є фізичними особами, що використовують системи ШІ в ході суто особистої непрофесійної діяльності.

11. Цей Регламент не перешкоджає Союзу або державам-членам підтримувати або вводити закони, нормативні акти або адміністративні положення, які є більш сприятливими для працівників з точки зору захисту їхніх прав щодо використання систем ШІ роботодавцями, або заохочувати або допускати застосування колективних угод, які є більш сприятливими для працівників.

12. Цей Регламент не застосовується до систем ШІ, що розповсюджуються під вільними ліцензіями з відкритим вихідним кодом, якщо вони не розміщуються на ринку або не вводяться в експлуатацію як високоризикові системи ШІ або як система ШІ, що підпадає під статтю 5 або 50.

Стаття 3

Визначення

Для цілей цього Регламенту застосовуються такі визначення:

(1)	«система ШІ» означає машинну систему, спроектовану для роботи з різними рівнями автономії та яка може виявляти адаптивність після розгортання, і яка, з явних або неявних цілей, виводить зі свого вхідного сигналу, як генерувати вихідні дані, наприклад прогнози, контент, рекомендації або рішення, що можуть впливати на фізичне або віртуальне середовище;
(2)	«ризик» означає поєднання ймовірності настання шкоди та тяжкості цієї шкоди;

(3) «постачальник» означає фізичну або юридичну особу, орган публічної влади, агентство або інший орган, що розробляє систему ШІ або загальноцільову модель ШІ або має розроблену систему ШІ або загальноцільову модель ШІ та розміщує її на ринку або вводить систему ШІ в експлуатацію під власним іменем або торговельною маркою, незалежно від того, чи є це платним або безкоштовним;

(4) «суб'єкт розгортання» означає фізичну або юридичну особу, орган публічної влади, агентство або інший орган, що використовує систему ШІ під своїм керівництвом, крім випадків, коли система ШІ використовується в ході особистої непрофесійної діяльності;

(5) «уповноважений представник» означає фізичну або юридичну особу, що розташована або заснована в Союзі та отримала та прийняла письмовий мандат від постачальника системи ШІ або загальноцільової моделі ШІ для виконання та здійснення від його імені відповідно зобов'язань та процедур, встановлених цим Регламентом;

(6) «імпортер» означає фізичну або юридичну особу, що розташована або заснована в Союзі та розміщує на ринку систему ШІ, що носить ім'я або торговельну марку фізичної або юридичної особи, заснованої в третій країні;

(7) «дистриб'ютор» означає фізичну або юридичну особу в ланцюжку постачання, відмінну від постачальника або імпортера, що робить систему ШІ доступною на ринку Союзу;

(8) «оператор» означає постачальника, виробника продукту, суб'єкта розгортання, уповноваженого представника, імпортера або дистриб'ютора;

(9) «розміщення на ринку» означає перше надання в розпорядження системи ШІ або загальноцільової моделі ШІ на ринку Союзу;

(10) «надання в розпорядження на ринку» означає постачання системи ШІ або загальноцільової моделі ШІ для поширення або використання на

ринку Союзу в ході комерційної діяльності, незалежно від того, чи є це оплатним або безкоштовним;

(11) «введення в експлуатацію» означає постачання системи ШІ для першого використання безпосередньо суб'єкту розгортання або для власного використання в Союзі за її передбаченим призначенням;

(12) «передбачене призначення» означає використання, для якого система ШІ призначена постачальником, включаючи конкретний контекст та умови використання, як зазначено в інформації, наданій постачальником в інструкціях з використання, рекламних або збутових матеріалах та заявах, а також у технічній документації;

(13) «розумно передбачуване неналежне використання» означає використання системи ШІ у спосіб, що не відповідає її передбаченому призначенню, але може виникнути внаслідок розумно передбачуваної поведінки людини або взаємодії з іншими системами, включаючи інші системи ШІ;

(14) «компонент безпеки» означає компонент продукту або системи ШІ, що виконує функцію безпеки для такого продукту або системи ШІ, або відмова або несправність якого загрожує здоров'ю та безпеці осіб або майну;

(15) «інструкції з використання» означають інформацію, надану постачальником для інформування суб'єкта розгортання, зокрема, про передбачене призначення та належне використання системи ШІ;

(16) «відкликання системи ШІ» означає будь-який захід, спрямований на досягнення повернення постачальнику або виведення з експлуатації або блокування використання системи ШІ, що була надана в розпорядження суб'єктам розгортання;

(17) «вилучення системи ШІ» означає будь-який захід, спрямований на запобігання наданню в розпорядження системи ШІ, що перебуває в ланцюжку постачання, на ринку;

(18) «продуктивність системи ШІ» означає здатність системи ШІ досягати свого передбаченого призначення;

(19) «нотифікуючий орган» означає національний орган, відповідальний за встановлення та здійснення необхідних процедур для оцінки, призначення та нотифікації органів оцінки відповідності та для їхнього моніторингу;

(20) «оцінка відповідності» означає процес демонстрації того, чи виконані вимоги, викладені в Главі III, Розділі 2 стосовно високоризикованої системи ШІ;

(21) «орган оцінки відповідності» означає орган, що виконує діяльність з оцінки відповідності третьою стороною, включаючи тестування, сертифікацію та інспекцію;

(22) «нотифікований орган» означає орган оцінки відповідності, нотифікований відповідно до цього Регламенту та іншого відповідного гармонізаційного законодавства Союзу;

(23) «суттєва модифікація» означає зміну системи ШІ після її розміщення на ринку або введення в експлуатацію, яка не передбачена або запланована у первинній оцінці відповідності, проведеній постачальником, і в результаті якої відповідність системи ШІ вимогам, викладеним у Главі III, Розділі 2, зачіпається або виникає модифікація передбаченого призначення, для якого систему ШІ було оцінено;

(24) «маркування CE» означає маркування, яким постачальник вказує, що система ШІ відповідає вимогам, викладеним у Главі III, Розділі 2 та іншому застосовному гармонізаційному законодавству Союзу, що передбачає його нанесення;

(25) «система постринкового моніторингу» означає всі заходи, що здійснюються постачальниками систем ШІ для збору та перегляду досвіду, отриманого від використання систем ШІ, що вони розміщують на ринку або вводять в експлуатацію, з метою визначення будь-якої необхідності негайного застосування будь-яких необхідних коригувальних або превентивних дій;

(26) «орган ринкового нагляду» означає національний орган, що здійснює діяльність та вживає заходів відповідно до Регламенту (ЄС) 2019/1020;

(27) «гармонізований стандарт» означає гармонізований стандарт, як визначено в статті 2(1), пункт (c), Регламенту (ЄС) № 1025/2012;

(28) «загальна специфікація» означає набір технічних специфікацій, як визначено в статті 2, пункт (4) Регламенту (ЄС) № 1025/2012, що надає засоби для виконання певних вимог, встановлених відповідно до цього Регламенту;

(29) «навчальні дані» означають дані, що використовуються для навчання системи ШІ шляхом підбору її параметрів, що підлягають навчанню;

(30) «валідаційні дані» означають дані, що використовуються для оцінки навченої системи ШІ та налаштування її параметрів, що не підлягають навчанню, та її процесу навчання, зокрема для запобігання недостатньому або надмірному навчанню;

(31) «набір валідаційних даних» означає окремий набір даних або частину навчального набору даних у вигляді фіксованого або змінного поділу;

(32) «тестові дані» означають дані, що використовуються для незалежної оцінки системи ШІ з метою підтвердження очікуваної продуктивності цієї системи до її розміщення на ринку або введення в експлуатацію;

(33) «вхідні дані» означають дані, надані системі ШІ або безпосередньо нею отримані, на основі яких система виробляє вихідні дані;

(34) «біометричні дані» означають персональні дані, що є результатом конкретної технічної обробки стосовно фізичних, фізіологічних або поведінкових характеристик фізичної особи, таких як зображення обличчя або дактилоскопічні дані;

(35) «біометрична ідентифікація» означає автоматизоване розпізнавання фізичних, фізіологічних, поведінкових або психологічних характеристик людини з метою встановлення особи фізичної особи шляхом порівняння біометричних даних цієї особи з біометричними даними осіб, що зберігаються в базі даних;

(36) «біометрична верифікація» означає автоматизовану перевірку у форматі «один до одного», включаючи автентифікацію, особи фізичних осіб шляхом порівняння їхніх біометричних даних із раніше наданими біометричними даними;

(37) «спеціальні категорії персональних даних» означають категорії персональних даних, зазначені в статті 9(1) Регламенту (ЄС) 2016/679, статті 10 Директиви (ЄС) 2016/680 та статті 10(1) Регламенту (ЄС) 2018/1725;

(38) «чутливі оперативні дані» означають оперативні дані, пов'язані з діяльністю з попередження, виявлення, розслідування або переслідування кримінальних правопорушень, розкриття яких могло б поставити під загрозу цілісність кримінального провадження;

(39) «система розпізнавання емоцій» означає систему ШІ для ідентифікації або виведення емоцій або намірів фізичних осіб на основі їхніх біометричних даних;

(40) «система біометричної категоризації» означає систему ШІ для відносення фізичних осіб до конкретних категорій на основі їхніх біометричних даних, якщо вона не є допоміжною до іншої комерційної послуги та суворо необхідною з об'єктивних технічних причин;

(41) «система дистанційної біометричної ідентифікації» означає систему ШІ для ідентифікації фізичних осіб без їхньої активної участі, як правило, на відстані шляхом порівняння біометричних даних особи з біометричними даними, що містяться в довідковій базі даних;

(42) «система дистанційної біометричної ідентифікації в режимі реального часу» означає систему дистанційної біометричної ідентифікації, де захоплення біометричних даних, порівняння та ідентифікація відбуваються без значної затримки, охоплюючи не лише миттєву ідентифікацію, але й обмежені короткі затримки для уникнення обходу;

(43) «система відкладеної дистанційної біометричної ідентифікації» означає систему дистанційної біометричної ідентифікації, відмінну від системи дистанційної біометричної ідентифікації в режимі реального часу;

(44) «загальнодоступний простір» означає будь-яке фізичне місце, що перебуває у публічній або приватній власності та доступне для невизначеної кількості фізичних осіб, незалежно від того, чи можуть застосовуватися певні умови для доступу, та незалежно від потенційних обмежень щодо місткості;

(45) «правоохоронний орган» означає:

(a) будь-який орган публічної влади, компетентний у сфері попередження, розслідування, виявлення або переслідування кримінальних правопорушень або виконання кримінальних покарань, включаючи захист від загроз суспільній безпеці та їх попередження; або

	(b)	будь-який інший орган або суб'єкт, якому законодавством держави-члена доручено здійснення публічної влади та публічних повноважень для цілей попередження, розслідування, виявлення або переслідування кримінальних правопорушень або виконання кримінальних покарань, включаючи захист від загроз суспільній безпеці та їх попередження;
(46)		«правоохоронна діяльність» означає діяльність, що здійснюється правоохоронними органами або від їхнього імені для попередження, розслідування, виявлення або переслідування кримінальних правопорушень або виконання кримінальних покарань, включаючи захист від загроз суспільній безпеці та їх попередження;
(47)		«Офіс ШІ» означає функцію Комісії щодо сприяння реалізації, моніторингу та нагляду за системами ШІ та загальноцільовими моделями ШІ, а також управлінню ШІ, передбачену Рішенням Комісії від 24 січня 2024 року; посилання в цьому Регламенті на Офіс ШІ тлумачаться як посилання на Комісію;
(48)		«національний компетентний орган» означає нотифікуючий орган або орган ринкового нагляду; щодо систем ШІ, що вводяться в експлуатацію або використовуються установами, агентствами, службами та органами Союзу, посилання в цьому Регламенті на національні компетентні органи або органи ринкового нагляду тлумачаються як посилання на Європейського наглядача із захисту даних;

(49) «серйозний інцидент» означає інцидент або несправність системи ШІ, що прямо або опосередковано призводить до будь-якого з такого:

(a) смерть особи або серйозна шкода здоров'ю особи;

(b) серйозне та незворотне порушення управління або функціонування критичної інфраструктури;

(c) порушення зобов'язань відповідно до законодавства Союзу, спрямованих на захист основних прав;

(d) серйозна шкода майну або навколишньому середовищу;

(50) «персональні дані» означають персональні дані, як визначено в статті 4, пункт (1), Регламенту (ЄС) 2016/679;

(51) «неперсональні дані» означають дані, відмінні від персональних даних, як визначено в статті 4, пункт (1), Регламенту (ЄС) 2016/679;

(52) «профілювання» означає профілювання, як визначено в статті 4, пункт (4), Регламенту (ЄС) 2016/679;

(53) «план тестування в реальних умовах» означає документ, що описує цілі, методологію, географічний, популяційний та часовий обсяг, моніторинг, організацію та проведення тестування в реальних умовах;

(54) «план пісочниці» означає документ, погоджений між постачальником-учасником та компетентним органом, що описує цілі, умови, терміни, методологію та вимоги до діяльності, що здійснюється в рамках пісочниці;

(55) «регуляторна пісочниця ШІ» означає контрольовану систему, створену компетентним органом, яка пропонує постачальникам або перспективним постачальникам систем ШІ можливість розробляти, навчати, валідувати та тестувати, де це доречно в реальних умовах, інноваційну систему ШІ відповідно до плану пісочниці протягом обмеженого часу під регуляторним наглядом;

(56) «освіченість у сфері ШІ» означає навички, знання та розуміння, що дозволяють постачальникам, суб'єктам розгортання та постраждалим особам, з урахуванням їхніх відповідних прав та зобов'язань у контексті цього Регламенту, здійснювати обґрунтоване розгортання систем ШІ, а також набувати обізнаності щодо можливостей та ризиків ШІ та можливої шкоди, яку він може заподіяти;

(57) «тестування в реальних умовах» означає тимчасове тестування системи ШІ за її передбаченим призначенням в реальних умовах поза лабораторією або іншим змодельованим середовищем з метою збору надійних та стійких даних, а також оцінки та верифікації відповідності системи ШІ вимогам цього Регламенту, і воно не кваліфікується як розміщення системи ШІ на ринку або введення її в експлуатацію у значенні цього Регламенту за умови виконання всіх умов, передбачених статтею 57 або 60;

(58) «суб'єкт» для цілей тестування в реальних умовах означає фізичну особу, яка бере участь у тестуванні в реальних умовах;

(59) «інформована згода» означає вільно надане, конкретне, однозначне та добровільне вираження суб'єктом свого бажання брати участь у конкретному тестуванні в реальних умовах після ознайомлення з усіма аспектами тестування, що мають значення для прийняття суб'єктом рішення про участь;

(60) «дипфейк» означає зображення, аудіо- або відеовміст, згенерований або маніпульований ШІ, що нагадує реальних осіб, об'єкти, місця,

суб'єкти або події та міг би помилково здатися особі автентичним або правдивим;

(61) «масове порушення» означає будь-яку дію або бездіяльність, що суперечить законодавству Союзу, яке захищає інтереси осіб і яка:

(a) завдала або, ймовірно, завдасть шкоди колективним інтересам осіб, що проживають принаймні у двох державах-членах, відмінних від держави-члена, в якій:

(i) дія або бездіяльність виникла або мала місце;

(ii) відповідний постачальник або, де це застосовно, його уповноважений представник розташований або заснований; або

(iii) суб'єкт розгортання заснований, коли порушення вчиняється

суб'єктом розгортання;

(b) завдала, завдає або, ймовірно, завдасть шкоди колективним інтересам осіб та має спільні риси, включаючи однакову незаконну практику або однаковий порушуваний інтерес, і відбувається одночасно, вчинена одним оператором, принаймні у трьох державах-членах;

(62) «критична інфраструктура» означає критичну інфраструктуру, як визначено в статті 2, пункт (4), Директиви (ЄС) 2022/2557;

(63) «загальноцільова модель ШІ» означає модель ШІ, включаючи ту, що навчена на великому обсязі даних з використанням самоконтрольованого навчання у масштабі, яка демонструє значну узагальненість та здатна компетентно виконувати широкий спектр різноманітних завдань незалежно від способу розміщення моделі на ринку та яка може бути інтегрована в різноманітні системи або застосунки нижньої ланки, за винятком моделей ШІ, що використовуються для дослідницьких, розробницьких або прототипних дій до їх розміщення на ринку;

(64) «можливості з високим впливом» означають можливості, що відповідають або перевищують можливості, зафіксовані в найбільш передових загальноцільових моделях ШІ;

(65) «системний ризик» означає ризик, що є характерним для можливостей з високим впливом загальноцільових моделей ШІ та має значний вплив на ринок Союзу через їхнє охоплення або через фактичні або розумно передбачувані негативні наслідки для

суспільного здоров'я, безпеки, суспільної безпеки, основних прав або суспільства в цілому, який може поширюватися у масштабі по всьому ланцюжку цінностей;

(66) «загальноцільова система ШІ» означає систему ШІ, засновану на загальноцільовій моделі ШІ та здатну слугувати різноманітним цілям як для прямого використання, так і для інтеграції в інші системи ШІ;

(67) «операція з плаваючою комою» означає будь-яку математичну операцію або присвоювання, що включає числа з плаваючою комою, які є підмножиною дійсних чисел, що зазвичай представлені на комп'ютерах цілим числом фіксованої точності, масштабованим цілочисельним показником ступеня фіксованої основи;

(68) «постачальник нижньої ланки» означає постачальника системи ШІ, включаючи загальноцільову систему ШІ, яка інтегрує модель ШІ, незалежно від того, чи надається модель ШІ ними самими та вертикально інтегрована або надається іншим суб'єктом на основі договірних відносин.

Стаття 4

Освіченість у сфері ШІ

Постачальники та суб'єкти розгортання систем ШІ вживають заходів для забезпечення, максимально можливою мірою, достатнього рівня освіченості у сфері ШІ свого персоналу та інших осіб, що займаються функціонуванням та використанням систем ШІ від їхнього імені, з урахуванням їхніх технічних знань, досвіду, освіти та навчання та контексту, в якому системи ШІ використовуватимуться, та з урахуванням осіб або груп осіб, щодо яких системи ШІ використовуватимуться.

ГЛАВА II

ЗАБОРОНЕНІ ПРАКТИКИ ШТУЧНОГО ІНТЕЛЕКТУ

Стаття 5

Заборонені практики ШІ

1. Такі практики ШІ забороняються:

(a) розміщення на ринку, введення в експлуатацію або використання системи ШІ, що застосовує сублімінальні техніки, що виходять за межі свідомості особи, або цілеспрямовані маніпулятивні або обманливі техніки, з метою або з ефектом суттєвого викривлення поведінки особи або групи осіб шляхом значного порушення їхньої здатності приймати обґрунтоване рішення, тим самим змушуючи їх приймати рішення, яке вони б інакше не прийняли, таким чином, що заподіює або, ймовірно, заподіє такій особі, іншій особі або групі осіб значну шкоду;

(b) розміщення на ринку, введення в експлуатацію або використання системи ШІ, що експлуатує будь-яку з вразливостей фізичної особи або конкретної групи осіб через їхній вік, інвалідність або конкретну соціальну чи економічну ситуацію, з метою або з ефектом суттєвого викривлення поведінки такої особи або особи, що належить до такої групи, у спосіб, що заподіює або, ймовірно, заподіє такій особі або іншій особі значну шкоду;

(c) розміщення на ринку, введення в експлуатацію або використання систем ШІ для оцінки або класифікації фізичних осіб або груп осіб протягом певного часового проміжку на основі їхньої соціальної поведінки або відомих, виведених або передбачених особистих чи особистісних характеристик, де соціальний рейтинг призводить до одного або обох із такого:

(i) шкідливого або несприятливого поводження з певними фізичними особами або групами осіб у соціальних контекстах, що не пов'язані з

контекстами, в яких дані були спочатку згенеровані або зібрані;

(ii) шкідливого або несприятливого поводження з певними фізичними особами або групами осіб, що є невиправданим або непропорційним їхній соціальній поведінці або її тяжкості;

(d) розміщення на ринку, введення в експлуатацію для цієї конкретної мети або використання системи ШІ для оцінки ризику фізичних осіб з метою оцінки або прогнозування ризику вчинення фізичною особою кримінального правопорушення, виключно на основі профілювання фізичної особи або оцінки її рис характеру та характеристик; ця заборона не застосовується до систем ШІ, що використовуються для підтримки людської оцінки причетності особи до злочинної діяльності, яка вже ґрунтується на об'єктивних та верифікованих фактах, безпосередньо пов'язаних зі злочинною діяльністю;

(e) розміщення на ринку, введення в експлуатацію для цієї конкретної мети або використання систем ШІ, що створюють або розширюють бази даних розпізнавання облич шляхом нецільового парсингу зображень облич з інтернету або відеозаписів відеоспостереження;

(f) розміщення на ринку, введення в експлуатацію для цієї конкретної мети або використання систем ШІ для виведення емоцій фізичної особи у сферах робочих місць та навчальних закладів, крім випадків, коли використання системи ШІ призначене для впровадження або розміщення на ринку з медичних міркувань або міркувань безпеки;

(g) розміщення на ринку, введення в експлуатацію для цієї конкретної мети або використання систем біометричної категоризації, що категоризують індивідуально фізичних осіб на

основі їхніх біометричних даних для дедукції або виведення їхньої раси, політичних поглядів, членства в профспілці, релігійних або філософських переконань, статевого життя або сексуальної орієнтації; ця заборона не охоплює будь-яке маркування або фільтрацію законно набутих наборів біометричних даних, таких як зображення, на основі біометричних даних або категоризацію біометричних даних у сфері правоохоронної діяльності;

(h) використання систем дистанційної біометричної ідентифікації «в режимі реального часу» в загальнодоступних просторах для цілей правоохоронної діяльності, якщо та тією мірою, якою таке використання є суворо необхідним для однієї з таких цілей:

(i) цілеспрямований пошук конкретних жертв викрадення, торгівлі людьми або сексуальної експлуатації людей, а також пошук зниклих безвісти осіб;

(ii) попередження конкретної, суттєвої та неминучої загрози життю або фізичній безпеці фізичних осіб або реальної та існуючої чи реальної та передбачуваної загрози терористичного нападу;

(iii) встановлення місця перебування або ідентифікація особи, яка підозрюється у вчиненні кримінального правопорушення, з метою проведення кримінального розслідування або переслідування або

виконання кримінального покарання за правопорушення, зазначені в Додатку II та карані у відповідній державі-члені позбавленням волі або наказом про затримання на максимальний строк не менше чотирьох років.

Пункт (h) першого підпараграфа не завдає шкоди статті 9 Регламенту (ЄС) 2016/679 щодо обробки біометричних даних для цілей, відмінних від правоохоронної діяльності.

2. Використання систем дистанційної біометричної ідентифікації «в режимі реального часу» в загальнодоступних просторах для цілей правоохоронної діяльності для будь-якої з цілей, зазначених у пункті 1, першому підпараграфі, пункт (h), здійснюється для цілей, зазначених у цьому пункті, лише для підтвердження особи конкретно виявленої особи, та враховує такі елементи:

(a) характер ситуації, що зумовлює можливе використання, зокрема тяжкість, ймовірність та масштаб шкоди, яка була б заподіяна, якби система не використовувалася;

(b) наслідки використання системи для прав та свобод усіх відповідних осіб, зокрема тяжкість, ймовірність та масштаб цих наслідків.

Крім того, використання систем дистанційної біометричної ідентифікації «в режимі реального часу» в загальнодоступних просторах для цілей правоохоронної діяльності для будь-якої з цілей, зазначених у пункті 1, першому підпараграфі, пункт (h), цієї статті відповідає необхідним та пропорційним гарантіям та умовам щодо використання відповідно до національного законодавства, що дозволяє таке використання, зокрема щодо часових, географічних та особистісних обмежень. Використання системи дистанційної біометричної ідентифікації «в режимі реального часу» в загальнодоступних просторах дозволяється лише якщо правоохоронний орган провів оцінку впливу на основні права, як передбачено статтею 27, та зареєстрував систему в базі даних ЄС відповідно до статті 49. Однак у належно обґрунтованих невідкладних випадках використання таких систем може бути розпочато без реєстрації в базі даних ЄС за умови, що така реєстрація буде завершена без невиправданої затримки.

3. Для цілей пункту 1, першого підпараграфа, пункту (h) та пункту 2 кожне використання в цілях правоохоронної діяльності системи дистанційної біометричної ідентифікації «в режимі реального часу» в загальнодоступних просторах підлягає попередньому дозволу, наданому судовим органом або незалежним адміністративним органом, рішення якого є обов'язковим, держави-члена, в якій відбуватиметься використання, виданому за мотивованим запитом та відповідно до детальних правил національного законодавства, зазначених у пункті 5. Однак у належно обґрунтованій невідкладній ситуації використання такої системи може бути розпочато без дозволу за умови, що такий дозвіл

запитується без невиправданої затримки, не пізніше ніж через 24 години. Якщо такий дозвіл відхиляється, використання негайно припиняється, а всі дані, а також результати та вихідні дані такого використання негайно відкидаються та видаляються.

Компетентний судовий орган або незалежний адміністративний орган, рішення якого є обов'язковим, надає дозвіл лише тоді, коли він переконаний на основі об'єктивних доказів або чітких ознак, наданих йому, що використання відповідної системи дистанційної біометричної ідентифікації «в режимі реального часу» є необхідним та пропорційним для досягнення однієї з цілей, зазначених у пункті 1, першому підпараграфі, пункт (h), як визначено в запиті, і, зокрема, залишається обмеженим лише тим, що є суворо необхідним щодо часового проміжку, а також географічного та особистісного обсягу. При прийнятті рішення щодо запиту цей орган враховує елементи, зазначені в пункті 2. Жодне рішення, що породжує несприятливі правові наслідки для особи, не може прийматися виключно на основі вихідних даних системи дистанційної біометричної ідентифікації «в режимі реального часу».

4. Без шкоди для пункту 3 кожне використання системи дистанційної біометричної ідентифікації «в режимі реального часу» в загальнодоступних просторах для цілей правоохоронної діяльності повідомляється відповідному органу ринкового нагляду та національному органу захисту даних відповідно до національних правил, зазначених у пункті 5. Повідомлення містить, як мінімум, інформацію, зазначену в пункті 6, та не включає чутливих оперативних даних.

5. Держава-член може прийняти рішення про надання можливості повного або часткового дозволу на використання систем дистанційної біометричної ідентифікації «в режимі реального часу» в загальнодоступних просторах для цілей правоохоронної діяльності в межах та за умов, перелічених у пункті 1, першому підпараграфі, пункт (h), та пунктах 2 та 3. Відповідні держави-члени встановлюють у своєму національному законодавстві необхідні детальні правила щодо запиту, видачі та здійснення, а також нагляду та звітування щодо дозволів, зазначених у пункті 3. Ці правила також конкретизують, щодо яких із цілей, перелічених у пункті 1, першому підпараграфі, пункт (h), включаючи які з кримінальних правопорушень, зазначених у пункті (h)(iii) цього положення, компетентні органи можуть бути уповноважені використовувати ці системи для цілей правоохоронної діяльності. Держави-члени повідомляють ці правила Комісії не пізніше ніж через 30 днів після їх прийняття. Держави-члени можуть вводити відповідно до законодавства Союзу більш обмежувальні закони щодо використання систем дистанційної біометричної ідентифікації.

6. Національні органи ринкового нагляду та національні органи захисту даних держав-членів, яким було повідомлено про використання систем дистанційної біометричної ідентифікації «в режимі реального часу» в загальнодоступних просторах для цілей правоохоронної діяльності відповідно до пункту 4, подають Комісії щорічні звіти про таке використання. Для цієї мети Комісія надає державам-членам та національним органам ринкового нагляду та захисту даних шаблон, включаючи інформацію про кількість рішень, прийнятих компетентними судовими органами або незалежним адміністративним органом, рішення якого є обов'язковим, за запитами щодо дозволів відповідно до пункту 3 та їхній результат.

7. Комісія публікує щорічні звіти про використання систем дистанційної біометричної ідентифікації в режимі реального часу в загальнодоступних просторах для цілей правоохоронної діяльності на основі агрегованих даних держав-членів на підставі щорічних звітів, зазначених у пункті 6. Такі щорічні звіти не включають чутливих оперативних даних відповідної правоохоронної діяльності.

8. Ця стаття не впливає на заборони, що застосовуються у випадках, коли практика ШІ порушує інше законодавство Союзу.

ГЛАВА III

ВИСОКОРИЗИКОВІ СИСТЕМИ ШТУЧНОГО ІНТЕЛЕКТУ

РОЗДІЛ 1

Класифікація систем штучного інтелекту як високоризикових

Стаття 6

Правила класифікації для високоризикованих систем ШІ

1. Незалежно від того, чи система ШІ розміщується на ринку або вводиться в експлуатацію окремо від продуктів, зазначених у пунктах (a) та (b), така система ШІ вважається високоризикованою, якщо виконуються обидві такі умови:

(a) система ШІ призначена для використання як компонент безпеки продукту або система ШІ сама є продуктом, охопленим гармонізаційним законодавством Союзу, переліченим у Додатку I;

(b) продукт, компонентом безпеки якого відповідно до пункту (a) є система ШІ, або сама система ШІ як продукт, зобов'язана пройти оцінку відповідності третьою стороною з метою розміщення на ринку або введення в експлуатацію такого продукту відповідно до гармонізаційного законодавства Союзу, переліченого у Додатку I.

2. На додаток до високоризикованих систем ШІ, зазначених у параграфі 1, системи ШІ, зазначені у Додатку III, вважаються високоризикованими.

3. Відступаючи від параграфа 2, система ШІ, зазначена у Додатку III, не вважається високоризикованою, якщо вона не становить значного ризику заподіяння шкоди здоров'ю, безпеці або основним правам фізичних осіб, в тому числі шляхом суттєвого невпливу на результат прийняття рішень.

Перший підпараграф застосовується, якщо виконується будь-яка з таких умов:

(a) система ШІ призначена для виконання вузького процедурного завдання;

(b) система ШІ призначена для покращення результату попередньо завершеної діяльності людини;

(c) система ШІ призначена для виявлення закономірностей прийняття рішень або відхилень від попередніх закономірностей прийняття рішень і не призначена для заміни або впливу на попередньо завершену оцінку людини без належного перегляду людиною; або

(d) система ШІ призначена для виконання підготовчого завдання до оцінки, що є актуальною для цілей випадків використання, перелічених у Додатку III.

Незважаючи на перший підпараграф, система ШІ, зазначена у Додатку III, завжди вважається високоризикованою, якщо система ШІ здійснює профілювання фізичних осіб.

4. Постачальник, який вважає, що система ШІ, зазначена у Додатку III, не є високоризикованою, документує свою оцінку до розміщення такої системи на ринку або введення в експлуатацію. Такий постачальник підлягає зобов'язанню щодо реєстрації, встановленому у статті 49(2). На запит національних компетентних органів постачальник надає документацію оцінки.

5. Комісія, після консультації з Європейською радою зі штучного інтелекту (далі — «Рада»), і не пізніше 2 лютого 2026 року надає настанови, що визначають практичне застосування цієї статті відповідно до статті 96, разом з вичерпним переліком практичних прикладів випадків використання систем ШІ, що є високоризикованими та не є високоризикованими.

6. Комісія уповноважена приймати делеговані акти відповідно до статті 97 для внесення змін до параграфа 3, другого підпараграфа, цієї статті шляхом додавання нових умов до тих, що в ньому встановлені, або їх зміни, за наявності конкретних та достовірних доказів існування систем ШІ, що підпадають під сферу дії Додатку III, але не становлять значного ризику заподіяння шкоди здоров'ю, безпеці або основним правам фізичних осіб.

7. Комісія приймає делеговані акти відповідно до статті 97 для внесення змін до параграфа 3, другого підпараграфа, цієї статті шляхом вилучення будь-яких умов, що в ньому встановлені, за наявності конкретних та достовірних доказів того, що це необхідно для підтримання рівня захисту здоров'я, безпеки та основних прав, передбаченого цим Регламентом.

8. Будь-яке внесення змін до умов, встановлених у параграфі 3, другому підпараграфі, прийняте відповідно до параграфів 6 та 7 цієї статті, не зменшує загального рівня захисту здоров'я, безпеки та основних прав, передбаченого цим Регламентом, та забезпечує узгодженість з делегованими актами, прийнятими відповідно до статті 7(1), та враховує ринкові та технологічні розробки.

Стаття 7

Зміни до Додатку III

1. Комісія уповноважена приймати делеговані акти відповідно до статті 97 для внесення змін до Додатку III шляхом додавання або зміни випадків використання високоризикованих систем ШІ, де виконуються обидві такі умови:

(a) системи ШІ призначені для використання в будь-якій з областей, перелічених у Додатку III;

(b) системи ШІ становлять ризик заподіяння шкоди здоров'ю та безпеці або негативний вплив на основні права, і такий ризик є еквівалентним ризику заподіяння шкоди або негативного впливу, що становлять уже зазначені у Додатку III високоризикові системи ШІ, або перевищує його.

2. При оцінці умови відповідно до параграфа 1, пункту (b), Комісія враховує такі критерії:

(a)	призначення системи ШІ;
(b)	ступінь використання системи ШІ або ймовірність її використання;
(c)	характер та обсяг даних, що обробляються та використовуються системою ШІ, зокрема чи обробляються спеціальні категорії персональних даних;
(d)	ступінь автономної дії системи ШІ та можливість для людини скасувати рішення або рекомендації, що можуть призвести до потенційної шкоди;
(e)	ступінь, до якого використання системи ШІ вже завдало шкоди здоров'ю та безпеці, мало негативний вплив на основні права або викликало значні занепокоєння щодо ймовірності такої шкоди або негативного впливу, що підтверджується, наприклад, звітами або задокументованими твердженнями, поданими до національних компетентних органів або іншими звітами, у відповідних випадках;
(f)	потенційний масштаб такої шкоди або такого негативного впливу, зокрема з точки зору його інтенсивності та здатності впливати на кількох осіб або непропорційно впливати на певну групу осіб;
(g)	ступінь залежності осіб, яким потенційно може бути завдана шкода або які зазнають негативного впливу, від результату, отриманого за допомогою системи ШІ, зокрема тому, що з практичних або правових причин неможливо розумно відмовитися від такого результату;
(h)	ступінь наявності дисбалансу влади або вразливості осіб, яким потенційно може бути завдана шкода або які зазнають негативного впливу, стосовно суб'єкта розгортання системи ШІ, зокрема через статус, повноваження, знання, економічні або соціальні обставини або вік;
(i)	ступінь, до якого результат, отриманий із залученням системи ШІ, легко піддається виправленню або скасуванню, з урахуванням технічних рішень, доступних для його

виправлення або скасування, при цьому результати, що мають негативний вплив на здоров'я, безпеку або основні права, не вважаються такими, що легко піддаються виправленню або скасуванню;

(j) масштаб та ймовірність вигоди від розгортання системи ШІ для окремих осіб, груп або суспільства в цілому, включаючи можливі вдосконалення безпеки продукту;

(k) ступінь, до якого чинне законодавство Союзу передбачає:

(i) ефективні засоби правового захисту щодо ризиків, що становлять системи ШІ, за виключенням вимог про відшкодування збитків;

(ii) ефективні заходи для запобігання таким ризикам або їх суттєвого мінімізування.

3. Комісія уповноважена приймати делеговані акти відповідно до статті 97 для внесення змін до переліку в Додатку III шляхом вилучення високоризикованих систем ШІ, де виконуються обидві такі умови:

(a) відповідна високоризикована система ШІ більше не становить жодних значних ризиків для основних прав, здоров'я або безпеки, з урахуванням критеріїв, перелічених у параграфі 2;

(b) вилучення не зменшує загального рівня захисту здоров'я, безпеки та основних прав відповідно до законодавства Союзу.

РОЗДІЛ 2

Вимоги до високоризикових систем штучного інтелекту

Стаття 8

Відповідність вимогам

1. Високоризиковані системи ШІ відповідають вимогам, викладеним у цьому Розділі, з урахуванням їхнього призначення, а також загальновизнаного стану мистецтва в галузі ШІ та технологій, пов'язаних із ШІ. Система управління ризиками, зазначена у статті 9, береться до уваги при забезпеченні відповідності цим вимогам.

2. Якщо продукт містить систему ШІ, до якої застосовуються як вимоги цього Регламенту, так і вимоги гармонізаційного законодавства Союзу, переліченого у Розділі А Додатку I, постачальники несуть відповідальність за забезпечення повної відповідності їхнього продукту всім застосовним вимогам відповідно до застосовного гармонізаційного законодавства Союзу. Забезпечуючи відповідність високоризикованих систем ШІ, зазначених у параграфі 1, вимогам, встановленим у цьому Розділі, та з метою забезпечення узгодженості, уникнення дублювання та мінімізування додаткового навантаження, постачальники мають право за потреби інтегрувати необхідні процеси тестування та звітності, інформацію та документацію, яку вони надають щодо свого продукту, до документації та процедур, що вже існують і вимагаються відповідно до гармонізаційного законодавства Союзу, переліченого у Розділі А Додатку I.

Стаття 9

Система управління ризиками

1. Щодо високоризикованих систем ШІ встановлюється, впроваджується, документується та підтримується система управління ризиками.

2. Система управління ризиками розуміється як безперервний ітеративний процес, що планується та здійснюється протягом усього життєвого циклу високоризикованої системи ШІ, що вимагає регулярного систематичного перегляду та оновлення. Вона охоплює такі кроки:

(a) ідентифікація та аналіз відомих та розумно передбачуваних ризиків, які високоризикована система ШІ може становити для здоров'я, безпеки або основних прав при використанні такої системи відповідно до її призначення;

(b) оцінка та визначення ризиків, що можуть виникнути при використанні високоризикованої системи ШІ відповідно до її призначення та за умов розумно передбачуваного неналежного використання;

(c) оцінка інших ризиків, що можуть виникнути, на основі аналізу даних, зібраних із системи постринкового моніторингу, зазначеної у статті 72;

(d) прийняття відповідних та цілеспрямованих заходів управління ризиками, призначених для усунення ризиків, ідентифікованих відповідно до пункту (a).

3. Ризики, зазначені у цій статті, стосуються лише тих, що можуть бути розумно пом'якшені або усунуті шляхом розробки або проектування високоризикованої системи ШІ або надання відповідної технічної інформації.

4. Заходи управління ризиками, зазначені у параграфі 2, пункті (d), належним чином враховують наслідки та можливу взаємодію, що виникають внаслідок спільного застосування вимог, викладених у цьому Розділі, з метою більш ефективного мінімізування ризиків при досягненні відповідного балансу при впровадженні заходів для виконання цих вимог.

5. Заходи управління ризиками, зазначені у параграфі 2, пункті (d), мають бути такими, щоб відповідний залишковий ризик, пов'язаний з кожною небезпекою, а також загальний залишковий ризик високоризикованих систем ШІ визнавалися прийнятними.

При визначенні найбільш відповідних заходів управління ризиками забезпечується таке:

(a) усунення або зменшення ризиків, ідентифікованих та оцінених відповідно до параграфа 2, настільки, наскільки це технічно можливо, шляхом відповідного проектування та розробки високоризикованої системи ШІ;

(b) у відповідних випадках, впровадження відповідних заходів пом'якшення та контролю, що стосуються ризиків, які не можуть бути усунуті;

(c) надання інформації, що вимагається відповідно до статті 13, та у відповідних випадках навчання суб'єктам розгортання.

З метою усунення або зменшення ризиків, пов'язаних з використанням високоризикованої системи ШІ, належним чином враховуються технічні знання, досвід, освіта, навчання, що очікується від суб'єкта розгортання, та передбачуваний контекст, у якому система призначена для використання.

6. Високоризиковані системи ШІ тестуються з метою визначення найбільш відповідних та цілеспрямованих заходів управління ризиками. Тестування забезпечує стабільну роботу високоризикованих систем ШІ відповідно до їхнього призначення та відповідність вимогам, встановленим у цьому Розділі.

7. Процедури тестування можуть включати тестування в реальних умовах відповідно до статті 60.

8. Тестування високоризикованих систем ШІ проводиться у відповідних випадках у будь-який час протягом процесу розробки і, у будь-якому разі, до їх розміщення на ринку або введення в експлуатацію. Тестування проводиться відповідно до попередньо визначених показників та імовірнісних порогів, що відповідають призначенню високоризикованої системи ШІ.

9. При впровадженні системи управління ризиками, передбаченої параграфами 1–7, постачальники враховують, чи з огляду на її призначення, ймовірно, що високоризикована система ШІ матиме негативний вплив на осіб, молодших 18 років, та у відповідних випадках на інші вразливі групи.

10. Для постачальників високоризикованих систем ШІ, що підпадають під вимоги щодо внутрішніх процесів управління ризиками відповідно до інших відповідних положень законодавства Союзу, аспекти, передбачені параграфами 1–9, можуть бути частиною процедур управління ризиками, встановлених відповідно до такого законодавства, або поєднуватися з ними.

Стаття 10

Дані та управління даними

1. Високоризиковані системи ШІ, що використовують методи, які передбачають навчання моделей ШІ на даних, розробляються на основі навчальних, валідаційних та тестових наборів даних, що відповідають критеріям якості, зазначеним у параграфах 2–5, у всіх випадках, коли такі набори даних використовуються.

2. Навчальні, валідаційні та тестові набори даних підлягають практикам управління та адміністрування даних, що відповідають призначенню високоризикованої системи ШІ. Такі практики стосуються зокрема:

(a) відповідних проектних рішень;

(b) процесів збору даних та походження даних, а у випадку персональних даних — первісної мети збору даних;

(c) відповідних операцій обробки для підготовки даних, таких як анотування, маркування, очищення, оновлення, збагачення та агрегування;

(d) формулювання припущень, зокрема щодо інформації, яку дані мають вимірювати та відображати;

(e) оцінки наявності, кількості та придатності необхідних наборів даних;

(f) вивчення з огляду на можливі упередженості, що можуть впливати на здоров'я та безпеку осіб, мати негативний вплив на основні права або призводити до дискримінації, забороненої законодавством Союзу, особливо там, де вихідні дані впливають на вхідні дані для майбутніх операцій;

(g) відповідних заходів для виявлення, запобігання та пом'якшення можливих упередженостей, визначених відповідно до пункту (f);

(h) виявлення відповідних прогалин або недоліків даних, що перешкоджають відповідності цьому Регламенту, та того, як такі прогалини та недоліки можуть бути усунуті.

3. Навчальні, валідаційні та тестові набори даних мають бути релевантними, достатньо репрезентативними та, наскільки це можливо, вільними від помилок і повними з огляду на призначення. Вони мають мати відповідні статистичні властивості, включаючи, де це застосовно, стосовно осіб або груп осіб, щодо яких призначена для використання високоризикована система ШІ. Такі характеристики наборів даних можуть задовольнятися на рівні окремих наборів даних або на рівні їх комбінації.

4. Набори даних враховують, тією мірою, яка вимагається призначенням, характеристики або елементи, що є особливими для конкретного географічного, контекстуального, поведінкового або функціонального середовища, в якому призначена для використання висококризована система ШІ.

5. Тією мірою, якою це суворо необхідно для цілей забезпечення виявлення та виправлення упередженостей стосовно високоризикованих систем ШІ відповідно до параграфа (2), пунктів (f) та (g) цієї статті, постачальники таких систем можуть у виняткових випадках обробляти спеціальні категорії персональних даних за умови відповідних гарантій основних прав і свобод фізичних осіб. Крім положень, викладених у Регламентах (ЄС) 2016/679 та (ЄС) 2018/1725 та Директиві (ЄС) 2016/680, для такої обробки мають виконуватися всі такі умови:

(a) виявлення та виправлення упередженостей не може бути ефективно здійснено шляхом обробки інших даних, включаючи синтетичні або анонімізовані дані;

(b) спеціальні категорії персональних даних підпадають під технічні обмеження щодо повторного використання персональних даних та найсучасніші заходи безпеки та захисту приватності, включаючи псевдонімізацію;

(c) спеціальні категорії персональних даних підпадають під заходи для забезпечення того, що оброблювані персональні дані захищені, охоронені, підлягають відповідним гарантіям, включаючи суворий контроль та документування доступу, для запобігання зловживанням та забезпечення того, що лише уповноважені особи мають доступ до цих персональних даних із відповідними зобов'язаннями щодо конфіденційності;

(d) спеціальні категорії персональних даних не передаються, не переносяться або не надаються для доступу іншим сторонам;

(e)	спеціальні категорії персональних даних видаляються після виправлення упередженості або по закінченні терміну зберігання персональних даних залежно від того, що настане раніше;
(f)	записи про діяльність з обробки відповідно до Регламентів (ЄС) 2016/679 та (ЄС) 2018/1725 та Директиви (ЄС) 2016/680 включають причини, з яких обробка спеціальних категорій персональних даних була суворо необхідною для виявлення та виправлення упередженостей, та чому ця мета не могла бути досягнута шляхом обробки інших даних.

6. Для розробки високоризикованих систем ШІ, що не використовують методи навчання моделей ШІ, параграфи 2–5 застосовуються лише до тестових наборів даних.

Стаття 11

Технічна документація

1. Технічна документація на високоризиковану систему ШІ складається до розміщення такої системи на ринку або введення в експлуатацію та підтримується в актуальному стані.

Технічна документація складається таким чином, щоб продемонструвати відповідність високоризикованої системи ШІ вимогам, викладеним у цьому Розділі, та надати національним компетентним органам та нотифікованим органам необхідну інформацію у чіткій та вичерпній формі для оцінки відповідності системи ШІ цим вимогам. Вона містить, як мінімум, елементи, встановлені в Додатку IV. МСП, включаючи стартапи, можуть надавати елементи технічної документації, зазначені в Додатку IV, у спрощений спосіб. З цією метою Комісія встановлює спрощену форму технічної документації, орієнтовану на потреби малих та мікропідприємств. Якщо МСП, включаючи стартап, вирішує надати інформацію, що вимагається в Додатку IV, у спрощений спосіб, воно використовує форму, зазначену в цьому параграфі. Нотифіковані органи приймають цю форму для цілей оцінки відповідності.

2. Якщо на ринок розміщується або вводиться в експлуатацію високоризикована система ШІ, що відноситься до продукту, охопленого гармонізаційним законодавством Союзу, переліченим у Розділі А Додатку I, складається єдиний комплект технічної документації, що містить всю інформацію, викладену в параграфі 1, а також інформацію, що вимагається відповідно до таких правових актів.

3. Комісія уповноважена приймати делеговані акти відповідно до статті 97 для внесення змін до Додатку IV, де це необхідно, щоб забезпечити, що з урахуванням технічного прогресу технічна документація надає всю інформацію, необхідну для оцінки відповідності системи вимогам, викладеним у цьому Розділі.

Стаття 12

Ведення записів

1. Високоризиковані системи ШІ технічно забезпечують автоматичне ведення записів подій (журналів) протягом строку служби системи.

2. З метою забезпечення рівня відстежуваності функціонування високоризикованої системи ШІ, що відповідає призначенню системи, можливості ведення журналів забезпечують фіксування подій, що стосуються:

(a) ідентифікації ситуацій, що можуть призвести до того, що високоризикована система ШІ становитиме ризик у значенні статті 79(1) або до суттєвої модифікації;

(b) сприяння постринковому моніторингу, зазначеному у статті 72; та

(c) моніторингу роботи високоризикованих систем ШІ, зазначених у статті 26(5).

3. Для високоризикованих систем ШІ, зазначених у пункті 1 (a) Додатку III, можливості ведення журналів забезпечують, як мінімум:

(a) фіксування часового проміжку кожного використання системи (дата і час початку та дата і час закінчення кожного використання);

(b) довідкову базу даних, з якою система звіряла вхідні дані;

(c) вхідні дані, для яких пошук призвів до збігу;

(d) ідентифікацію фізичних осіб, залучених до перевірки результатів, як зазначено у статті 14(5).

Стаття 13

Прозорість та надання інформації суб'єктам розгортання

1. Високоризиковані системи ШІ проектуються та розробляються таким чином, щоб забезпечити достатню прозорість їх функціонування, що дозволяє суб'єктам розгортання інтерпретувати вихідні дані системи та відповідно їх використовувати. Забезпечується відповідний тип і ступінь прозорості з метою дотримання відповідних зобов'язань постачальника та суб'єкта розгортання, встановлених у Розділі 3.

2. Високоризиковані системи ШІ супроводжуються інструкціями з використання у відповідному цифровому форматі або в іншому вигляді, що містять стислу, повну, правильну та чітку інформацію, яка є релевантною, доступною та зрозумілою для суб'єктів розгортання.

3. Інструкції з використання містять принаймні таку інформацію:

(a) найменування та контактні дані постачальника і, де це застосовно, його уповноваженого представника;

(b) характеристики, можливості та обмеження продуктивності високоризикованої системи ШІ, включаючи:

(i) її призначення;

(ii) рівень точності, включаючи її показники, надійність та кібербезпеку, зазначені у статті 15, відповідно до яких висококризикована система ШІ була протестована та валідована і яких можна очікувати, а також будь-які відомі та передбачувані обставини, що можуть вплинути на очікуваний рівень точності, надійності та кібербезпеки;

(iii) будь-які відомі або передбачувані обставини, пов'язані з використанням високоризикованої системи ШІ відповідно до її призначення або за умов розумно передбачуваного неналежного використання, які можуть призвести до ризиків для здоров'я та безпеки або основних прав, зазначених у статті 9(2);

(iv) де це застосовно, технічні можливості та характеристики високоризикованої системи ШІ для надання інформації,

що є релевантною для пояснення її вихідних даних;

(v) у відповідних випадках, її продуктивність щодо конкретних осіб або груп осіб, для яких система призначена для використання;

(vi) у відповідних випадках, специфікації для вхідних даних або будь-яку іншу релевантну інформацію щодо навчальних, валідаційних та тестових наборів даних, що використовуються, з урахуванням призначення високоризикованої системи ШІ;

(vii) де це застосовно, інформацію, що дозволяє суб'єктам розгортання інтерпретувати вихідні дані високоризикованої системи ШІ та використовувати їх належним чином;

(c) зміни до високоризикованої системи ШІ та її продуктивності, що були попередньо визначені постачальником на момент первинної оцінки відповідності, якщо такі є;

(d) заходи людського нагляду, зазначені у статті 14, включаючи технічні заходи, що вживаються для полегшення інтерпретації вихідних даних високоризикованих систем ШІ суб'єктами розгортання;

(e) обчислювальні та апаратні ресурси, що необхідні, очікуваний строк служби високоризикованої системи ШІ та будь-які необхідні заходи технічного обслуговування та догляду, включаючи їхню частоту, для забезпечення належного функціонування такої системи ШІ, в тому числі щодо оновлень програмного забезпечення;

(f) де це доречно, опис механізмів, що включені до складу високоризикованої системи ШІ і що дозволяють суб'єктам розгортання належним чином збирати, зберігати та інтерпретувати журнали відповідно до статті 12.

Стаття 14

Людський нагляд

1. Високоризиковані системи ШІ проектуються та розробляються таким чином, в тому числі із застосуванням відповідних засобів людино-машинного інтерфейсу, щоб вони могли бути ефективно піддані нагляду з боку фізичних осіб протягом часу їхнього використання.

2. Людський нагляд спрямований на запобігання або мінімізування ризиків для здоров'я, безпеки або основних прав, що можуть виникнути при використанні високоризикованої системи ШІ відповідно до її призначення або за умов розумно передбачуваного неналежного використання, зокрема там, де такі ризики зберігаються незважаючи на застосування інших вимог, встановлених у цьому Розділі.

3. Заходи нагляду є співмірними з ризиками, рівнем автономності та контекстом використання високоризикованої системи ШІ та забезпечуються одним або обома з таких типів заходів:

(a) заходи, визначені та вбудовані, коли це технічно можливо, до високоризикованої системи ШІ постачальником до її розміщення на ринку або введення в експлуатацію;

(b) заходи, визначені постачальником до розміщення високоризикованої системи ШІ на ринку або введення її в експлуатацію та що є відповідними для впровадження суб'єктом розгортання.

4. Для цілей впровадження параграфів 1, 2 та 3 висококризикована система ШІ надається суб'єкту розгортання таким чином, щоб фізичні особи, яким призначений людський нагляд, могли у відповідних та пропорційних випадках:

(a) належним чином розуміти відповідні можливості та обмеження високоризикованої системи ШІ та бути здатними належно контролювати її роботу, в тому числі з метою виявлення та усунення аномалій, збоїв та неочікуваної продуктивності;

(b) зберігати обізнаність про можливу тенденцію автоматичного покладання або надмірного покладання на вихідні дані, вироблені високоризикованою системою ШІ (автоматизована упередженість), зокрема для високоризикованих систем ШІ, що використовуються для надання інформації або рекомендацій для рішень, що мають прийматися фізичними особами;

(c) правильно інтерпретувати вихідні дані високоризикованої системи ШІ, з урахуванням, наприклад, наявних засобів та методів інтерпретації;

(d) вирішувати у будь-якій конкретній ситуації не використовувати високоризиковану систему ШІ або ігнорувати, скасовувати або відхиляти вихідні дані такої системи;

(e) втручатися в роботу високоризикованої системи ШІ або переривати роботу системи за допомогою кнопки «стоп» або аналогічної процедури, що дозволяє системі зупинитися у безпечному стані.

5. Для високоризикованих систем ШІ, зазначених у пункті 1(a) Додатку III, заходи, зазначені у параграфі 3 цієї статті, є такими, щоб забезпечити, що крім того, жодна дія або рішення не вживаються суб'єктом розгортання на підставі ідентифікації, отриманої в результаті роботи системи, якщо така ідентифікація не була окремо перевірена та підтверджена принаймні двома фізичними особами з необхідною компетентністю, підготовкою та повноваженнями.

Вимога про окрему перевірку принаймні двома фізичними особами не застосовується до високоризикованих систем ШІ, що використовуються для цілей правоохоронної діяльності, міграції, контролю кордонів або притулку, де законодавство Союзу або національне законодавство вважає застосування цієї вимоги непропорційним.

Стаття 15

Точність, надійність та кібербезпека

1. Високоризиковані системи ШІ проектуються та розробляються таким чином, щоб вони досягали відповідного рівня точності, надійності та кібербезпеки та стабільно функціонували у цих аспектах протягом усього їхнього життєвого циклу.

2. Для вирішення технічних аспектів того, як вимірювати відповідні рівні точності та надійності, встановлені у параграфі 1, та будь-які інші релевантні показники ефективності, Комісія у співпраці з відповідними зацікавленими сторонами та організаціями, такими як органи з метрології та порівняльного аналізу, заохочує у відповідних випадках розробку еталонів та методологій вимірювання.

3. Рівні точності та відповідні показники точності високоризикованих систем ШІ зазначаються в інструкціях з використання, що додаються.

4. Високоризиковані системи ШІ мають бути настільки стійкими, наскільки це можливо, щодо помилок, несправностей або невідповідностей, що можуть виникати в системі або в середовищі, в якому функціонує система, зокрема через їхню взаємодію з фізичними особами або іншими системами. Щодо цього вживаються технічні та організаційні заходи.

Надійність високоризикованих систем ШІ може досягатися шляхом технічних рішень з резервуванням, що можуть включати резервні або відмовостійкі плани.

Високоризиковані системи ШІ, що продовжують навчатися після розміщення на ринку або введення в експлуатацію, розробляються таким чином, щоб усунути або максимально зменшити ризик того, що можливо упереджені вихідні дані впливатимуть на вхідні дані для майбутніх операцій (петлі зворотного зв'язку), та щоб забезпечити, що будь-які такі петлі зворотного зв'язку належним чином усуваються за допомогою відповідних пом'якшувальних заходів.

5. Високоризиковані системи ШІ мають бути стійкими до спроб неуповноважених третіх сторін змінити їхнє використання, вихідні дані або продуктивність шляхом використання вразливостей системи.

Технічні рішення, що спрямовані на забезпечення кібербезпеки високоризикованих систем ШІ, мають відповідати відповідним обставинам та ризикам.

Технічні рішення для усунення специфічних вразливостей ШІ включають, де це доречно, заходи для запобігання, виявлення, реагування, вирішення та контролю атак, що намагаються маніпулювати навчальним набором даних (отруєння даних) або попередньо навченими компонентами, що використовуються в навчанні (отруєння моделі), вхідних даних, призначених для того, щоб змусити модель ШІ зробити помилку (змагальні приклади або уникнення моделі), атак на конфіденційність або вад моделі.

РОЗДІЛ 3

Зобов'язання постачальників і суб'єктів розгортання високоризикових систем штучного інтелекту та інших сторін

Стаття 16

Зобов'язання постачальників високоризикованих систем ШІ

Постачальники високоризикованих систем ШІ:

(a)	забезпечують відповідність своїх високоризикованих систем ШІ вимогам, викладеним у Розділі 2;
(b)	зазначають на високоризикованій системі ШІ або, де це неможливо, на її упаковці або супровідній документації, залежно від обставин, своє ім'я, зареєстровану торгову назву або зареєстровану торговельну марку, адресу, за якою з ними можна зв'язатися;
(c)	мають систему управління якістю, що відповідає статті 17;
(d)	зберігають документацію, зазначену у статті 18;
(e)	за умови контролю над ними, зберігають журнали, автоматично згенеровані їхніми високоризикованими системами ШІ, як зазначено у статті 19;
(f)	забезпечують проходження відповідної процедури оцінки відповідності, зазначеної у статті 43, до розміщення на ринку або введення в експлуатацію;
(g)	складають декларацію відповідності ЄС відповідно до статті 47;
(h)	наносять маркування CE на високоризикову систему ШІ або, де це неможливо, на її упаковку або супровідну документацію для підтвердження відповідності цьому Регламенту відповідно до статті 48;
(i)	дотримуються реєстраційних зобов'язань, зазначених у статті 49(1);

(j) вживають необхідних коригувальних заходів та надають інформацію, як того вимагає стаття 20;

(k) на обґрунтований запит національного компетентного органу демонструють відповідність високоризикованої системи ШІ вимогам, викладеним у Розділі 2;

(l) забезпечують відповідність високоризикованої системи ШІ вимогам доступності відповідно до Директив (ЄС) 2016/2102 та (ЄС) 2019/882.

Стаття 17

Система управління якістю

1. Постачальники високоризикованих систем ШІ запроваджують систему управління якістю, що забезпечує відповідність цьому Регламенту. Така система документується систематично та впорядковано у формі письмових політик, процедур та інструкцій та охоплює принаймні такі аспекти:

(a) стратегію дотримання нормативно-правових вимог, включаючи відповідність процедурам оцінки відповідності та процедурам управління змінами до високоризикованої системи ШІ;

(b) методи, процедури та систематичні дії, що застосовуються для проектування, контролю проектування та верифікації проекту високоризикованої системи ШІ;

(c) методи, процедури та систематичні дії, що застосовуються для розробки, контролю якості та забезпечення якості високоризикованої системи ШІ;

(d) процедури перевірки, тестування та валідації, що мають проводитися до, під час і після розробки високоризикованої системи ШІ, та частота, з якою вони мають проводитися;

(e) технічні специфікації, включаючи стандарти, що мають застосовуватися, і де відповідні гармонізовані стандарти не застосовуються повністю або не охоплюють усіх відповідних вимог, встановлених у Розділі 2, засоби, що мають використовуватися для забезпечення відповідності високоризикованої системи ШІ таким вимогам;

(f) системи та процедури управління даними, включаючи збір даних, накопичення даних, аналіз даних, маркування даних, зберігання даних, фільтрацію даних, видобування даних, агрегування даних, збереження даних та будь-яку іншу операцію з даними, що виконується до і з метою розміщення на ринку або введення в експлуатацію високоризикованих систем ШІ;

(g) систему управління ризиками, зазначену у статті 9;

(h) створення, впровадження та підтримку системи постринкового моніторингу відповідно до статті 72;

(i) процедури, пов'язані зі звітуванням про серйозні інциденти відповідно до статті 73;

(j) здійснення комунікації з національними компетентними органами, іншими відповідними органами, включаючи ті, що забезпечують або підтримують доступ до даних, нотифікованими органами, іншими операторами, замовниками або іншими зацікавленими сторонами;

(k) системи та процедури ведення записів всієї відповідної документації та інформації;

(l) управління ресурсами, включаючи заходи, пов'язані з безпекою постачання;

(m) систему підзвітності, що встановлює відповідальність керівництва та іншого персоналу щодо всіх аспектів, перелічених у цьому параграфі.

2. Впровадження аспектів, зазначених у параграфі 1, є пропорційним розміру організації постачальника. Постачальники в будь-якому разі дотримуються ступеня суворості та рівня захисту, що необхідні для забезпечення відповідності їхніх високоризикованих систем ШІ цьому Регламенту.

3. Постачальники високоризикованих систем ШІ, що підпадають під зобов'язання щодо систем управління якістю або еквівалентної функції відповідно до відповідного галузевого законодавства Союзу, можуть включати аспекти, перелічені у параграфі 1, до складу систем управління якістю відповідно до такого законодавства.

4. Для постачальників, що є фінансовими установами, які підпадають під вимоги щодо їхнього внутрішнього управління, угод або процесів відповідно до законодавства Союзу про фінансові послуги, зобов'язання щодо запровадження системи управління якістю, за винятком параграфа 1,

пунктів (g), (h) та (i) цієї статті, вважається виконаним шляхом дотримання правил щодо угод або процесів внутрішнього управління відповідно до відповідного законодавства Союзу про фінансові послуги. З цією метою враховуються будь-які гармонізовані стандарти, зазначені у статті 40.

Стаття 18

Зберігання документації

1. Постачальник зберігає у розпорядженні національних компетентних органів протягом 10 років після розміщення на ринку або введення в експлуатацію висококризикованої системи ШІ:

(a)	технічну документацію, зазначену у статті 11;
(b)	документацію щодо системи управління якістю, зазначеної у статті 17;
(c)	документацію щодо змін, схвалених нотифікованими органами, де це застосовно;
(d)	рішення та інші документи, видані нотифікованими органами, де це застосовно;
(e)	декларацію відповідності ЄС, зазначену у статті 47.

2. Кожна держава-член визначає умови, за яких документація, зазначена у параграфі 1, залишається у розпорядженні національних компетентних органів протягом строку, зазначеного у цьому параграфі, у випадках, коли постачальник або його уповноважений представник, зареєстрований на її території, збанкрутував або припинив свою діяльність до закінчення цього строку.

3. Постачальники, що є фінансовими установами, які підпадають під вимоги щодо їхнього внутрішнього управління, угод або процесів відповідно до законодавства Союзу про фінансові послуги, підтримують технічну документацію як частину документації, що зберігається відповідно до відповідного законодавства Союзу про фінансові послуги.

Стаття 19

Автоматично згенеровані журнали

1. Постачальники високоризикованих систем ШІ зберігають журнали, зазначені у статті 12(1), автоматично згенеровані їхніми висококризикованими системами ШІ, тією мірою, якою такі журнали перебувають під їхнім контролем. Без шкоди для застосовного законодавства Союзу або національного законодавства, журнали зберігаються протягом строку, що відповідає призначенню висококризикованої системи ШІ, щонайменше шість місяців, якщо інше не передбачено застосовним законодавством Союзу або національним законодавством, зокрема законодавством Союзу про захист персональних даних.

2. Постачальники, що є фінансовими установами, які підпадають під вимоги щодо їхнього внутрішнього управління, угод або процесів відповідно до законодавства Союзу про фінансові послуги, підтримують журнали, автоматично згенеровані їхніми висококризикованими системами ШІ, як частину документації, що зберігається відповідно до відповідного законодавства про фінансові послуги.

Стаття 20

Коригувальні заходи та обов'язок надання інформації

1. Постачальники високоризикованих систем ШІ, які вважають або мають підстави вважати, що висококризикована система ШІ, яку вони розмістили на ринку або ввели в експлуатацію, не відповідає цьому Регламенту, негайно вживають необхідних коригувальних заходів для приведення такої системи у відповідність, відкликання її з ринку, відключення або відзиву, залежно від обставин. Вони відповідно інформують дистриб'юторів відповідної висококризикованої системи ШІ та, де це застосовно, суб'єктів розгортання, уповноваженого представника та імпортерів.

2. Якщо висококризикована система ШІ становить ризик у значенні статті 79(1) і постачальник дізнається про такий ризик, він негайно розслідує причини у співпраці із суб'єктом розгортання, що подав звіт, де це застосовно, та інформує органи ринкового нагляду, компетентні для відповідної висококризикованої системи ШІ, та, де це застосовно, нотифікований орган, що видав сертифікат для такої висококризикованої системи ШІ відповідно до статті 44, зокрема, про характер невідповідності та будь-які відповідні коригувальні заходи, що були вжиті.

Стаття 21

Співпраця з компетентними органами

1. Постачальники високоризикованих систем ШІ на обґрунтований запит компетентного органу надають такому органу всю інформацію та документацію, необхідну для підтвердження відповідності висококризикованої системи ШІ вимогам, викладеним у Розділі 2, мовою, яку орган може легко зрозуміти, однією з офіційних мов інститутів Союзу, зазначених відповідною державою-членом.

2. На обґрунтований запит компетентного органу постачальники також надають компетентному органу, що зробив запит, у відповідних випадках доступ до автоматично згенерованих журналів висококризикованої системи ШІ, зазначених у статті 12(1), тією мірою, якою такі журнали перебувають під їхнім контролем.

3. Будь-яка інформація, отримана компетентним органом відповідно до цієї статті, обробляється відповідно до зобов'язань щодо конфіденційності, встановлених у статті 78.

Стаття 22

Уповноважені представники постачальників високоризикованих систем ШІ

1. До надання своїх висококризикованих систем ШІ на ринку Союзу постачальники, засновані в третіх країнах, шляхом письмового доручення призначають уповноваженого представника, заснованого в Союзі.

2. Постачальник забезпечує можливість свого уповноваженого представника виконувати завдання, зазначені в дорученні, отриманому від постачальника.

3. Уповноважений представник виконує завдання, зазначені в дорученні, отриманому від постачальника. На запит він надає копію доручення органам ринкового нагляду однією з офіційних мов інститутів Союзу, зазначених компетентним органом. Для цілей цього Регламенту доручення уповноважує уповноваженого представника на виконання таких завдань:

(a) перевіряти, що декларація відповідності ЄС, зазначена у статті 47, та технічна документація, зазначена у статті 11, були складені та що

відповідна процедура оцінки відповідності була проведена постачальником;

(b) зберігати у розпорядженні компетентних органів та національних органів або установ, зазначених у статті 74(10), протягом 10 років після розміщення висококризикованої системи ШІ на ринку або введення в експлуатацію, контактні дані постачальника, який призначив уповноваженого представника, копію декларації відповідності ЄС, зазначеної у статті 47, технічну документацію і, якщо це застосовно, сертифікат, виданий нотифікованим органом;

(c) надавати компетентному органу на обґрунтований запит всю інформацію та документацію, включаючи ту, що зазначена у пункті (b) цього підпараграфа, необхідну для підтвердження відповідності висококризикованої системи ШІ вимогам, викладеним у Розділі 2, включаючи доступ до журналів, зазначених у статті 12(1), автоматично згенерованих висококризикованою системою ШІ, тією мірою, якою такі журнали перебувають під контролем постачальника;

(d) співпрацювати з компетентними органами на обґрунтований запит у будь-яких заходах, що вживаються ними стосовно висококризикованої системи ШІ, зокрема для зменшення та пом'якшення ризиків, що становить висококризикована система ШІ;

(e) де це застосовно, дотримуватися реєстраційних зобов'язань, зазначених у статті 49(1), або, якщо реєстрація здійснюється самим постачальником, забезпечити правильність інформації, зазначеної у пункті 3 Розділу A Додатку VIII.

Доручення уповноважує уповноваженого представника звертатися до нього компетентними органами на додаток до постачальника або замість нього з усіх питань, пов'язаних із забезпеченням відповідності цьому Регламенту.

4. Уповноважений представник припиняє дію доручення, якщо він вважає або має підстави вважати, що постачальник діє всупереч своїм зобов'язанням відповідно до цього Регламенту. У такому випадку він негайно інформує відповідний орган ринкового нагляду, а також, де це застосовно, відповідний нотифікований орган про припинення дії доручення та про причини цього.

Стаття 23

Зобов'язання імпортерів

1. До розміщення висококризикованої системи ШІ на ринку імпортери забезпечують відповідність системи цьому Регламенту шляхом перевірки того, що:

(a)	відповідна процедура оцінки відповідності, зазначена у статті 43, була проведена постачальником висококризикованої системи ШІ;
(b)	постачальник склав технічну документацію відповідно до статті 11 та Додатку IV;
(c)	система несе необхідне маркування CE та супроводжується декларацією відповідності ЄС, зазначеною у статті 47, та інструкціями з використання;
(d)	постачальник призначив уповноваженого представника відповідно до статті 22(1).

2. Якщо імпортер має достатні підстави вважати, що висококризикована система ШІ не відповідає цьому Регламенту, або є підробленою, або супроводжується підробленою документацією, він не розміщує систему на ринку до приведення її у відповідність. Якщо висококризикована система ШІ становить ризик у значенні статті 79(1), імпортер інформує про це постачальника системи, уповноваженого представника та органи ринкового нагляду.

3. Імпортери зазначають своє ім'я, зареєстровану торгову назву або зареєстровану торговельну марку та адресу, за якою з ними можна зв'язатися, на висококризикованій системі ШІ та на її упаковці або супровідній документації, де це застосовно.

4. Імпортери забезпечують, що, поки висококризикована система ШІ перебуває під їхньою відповідальністю, умови зберігання або транспортування, де це застосовно, не загрожують її відповідності вимогам, викладеним у Розділі 2.

5. Імпортери зберігають протягом 10 років після розміщення висококризикованої системи ШІ на ринку або введення в експлуатацію копію сертифіката, виданого нотифікованим органом, де це застосовно, інструкцій з використання та декларації відповідності ЄС, зазначеної у статті 47.

6. Імпортери надають відповідним компетентним органам на обґрунтований запит всю необхідну інформацію та документацію, включаючи ту, що зазначена у параграфі 5, для підтвердження відповідності висококризикованої системи ШІ вимогам, викладеним у Розділі 2, мовою, яку вони можуть легко зрозуміти. З цією метою вони також забезпечують, що технічна документація може бути надана таким органам.

7. Імпортери співпрацюють з відповідними компетентними органами у будь-яких заходах, що вживаються такими органами стосовно висококризикованої системи ШІ, розміщеної на ринку імпортерами, зокрема для зменшення та пом'якшення ризиків, що нею становляться.

Стаття 24

Зобов'язання дистриб'юторів

1. До надання висококризикованої системи ШІ на ринку дистриб'ютори перевіряють, що вона несе необхідне маркування СЕ, що вона супроводжується копією декларації відповідності ЄС, зазначеної у статті 47, та інструкціями з використання, і що постачальник та імпортер такої системи, залежно від обставин, виконали свої відповідні зобов'язання, встановлені у статті 16, пунктах (b) та (c), та статті 23(3).

2. Якщо дистриб'ютор вважає або має підстави вважати на основі наявної у нього інформації, що висококризикована система ШІ не відповідає вимогам, викладеним у Розділі 2, він не надає висококризикову систему ШІ на ринку до приведення системи у відповідність з такими вимогами. Крім того, якщо висококризикована система ШІ становить ризик у значенні статті 79(1), дистриб'ютор інформує про це постачальника або імпортера системи, залежно від обставин.

3. Дистриб'ютори забезпечують, що, поки висококризикована система ШІ перебуває під їхньою відповідальністю, умови зберігання або транспортування, де це застосовно, не загрожують відповідності системи вимогам, викладеним у Розділі 2.

4. Дистриб'ютор, який вважає або має підстави вважати на основі наявної у нього інформації, що висококризикована система ШІ, яку він надав на ринку, не відповідає вимогам, викладеним у Розділі 2, вживає коригувальних заходів, необхідних для приведення такої системи у відповідність з такими вимогами, відкликання її з ринку або відзиву, або забезпечує, що постачальник, імпортер або будь-який відповідний оператор, залежно від обставин, вживає таких коригувальних заходів. Якщо висококризикована система ШІ становить ризик у значенні статті 79(1), дистриб'ютор негайно інформує постачальника або імпортера системи та органи, компетентні для відповідної висококризикованої системи ШІ, надаючи деталі, зокрема, щодо невідповідності та будь-яких вжитих коригувальних заходів.

5. На обґрунтований запит відповідного компетентного органу дистриб'ютори висококризикованої системи ШІ надають такому органу всю інформацію та документацію щодо своїх дій відповідно до параграфів 1–4, необхідну для підтвердження відповідності такої системи вимогам, викладеним у Розділі 2.

6. Дистриб'ютори співпрацюють з відповідними компетентними органами у будь-яких заходах, що вживаються такими органами стосовно висококризикованої системи ШІ, наданої на ринку дистриб'юторами, зокрема для зменшення або пом'якшення ризику, що нею становиться.

Стаття 25

Відповідальності в ланцюжку створення вартості ШІ

1. Будь-який дистриб'ютор, імпортер, суб'єкт розгортання або інша третя сторона вважається постачальником висококризикованої системи ШІ для цілей цього Регламенту та підпадає під зобов'язання постачальника відповідно до статті 16 за будь-якої з таких обставин:

(a) вони розміщують своє ім'я або торговельну марку на висококризикованій системі ШІ, що вже розміщена на ринку або введена в експлуатацію, без шкоди для контрактних угод, що передбачають інший розподіл зобов'язань;

(b) вони вносять суттєву модифікацію до висококризикованої системи ШІ, що вже була розміщена на ринку або вже була введена в експлуатацію таким чином, що вона залишається висококризикованою системою ШІ відповідно до статті 6;

(c) вони змінюють призначення системи ШІ, включаючи загальноцільову систему ШІ, яка не була класифікована як висококризикована та вже була розміщена на ринку або введена в експлуатацію таким чином, що відповідна система ШІ стає висококризикованою системою ШІ відповідно до статті 6.

2. У разі настання обставин, зазначених у параграфі 1, постачальник, який спочатку розмістив систему ШІ на ринку або ввів її в експлуатацію, більше не вважається постачальником такої конкретної системи ШІ для цілей цього Регламенту. Такий початковий постачальник тісно співпрацює з новими постачальниками та надає необхідну інформацію і забезпечує розумно очікуваний технічний доступ та іншу підтримку, що необхідні для виконання зобов'язань, встановлених у цьому Регламенті, зокрема щодо відповідності оцінці відповідності висококризикованих систем ШІ. Цей параграф не застосовується у випадках, коли початковий постачальник чітко зазначив, що його систему ШІ не слід перетворювати на висококризикову систему ШІ і, отже, вона не підпадає під зобов'язання щодо передачі документації.

3. У випадку висококризикованих систем ШІ, що є компонентами безпеки продуктів, охоплених гармонізаційним законодавством Союзу, переліченим у Розділі А Додатку I, виробник продукту вважається постачальником висококризикованої системи ШІ та підпадає під зобов'язання відповідно до статті 16 за будь-якої з таких обставин:

(a) висококризикована система ШІ розміщується на ринку разом з продуктом під ім'ям або торговельною маркою виробника продукту;

(b) висококризикована система ШІ вводиться в експлуатацію під ім'ям або торговельною маркою виробника продукту після розміщення продукту на ринку.

4. Постачальник висококризикованої системи ШІ та третя сторона, яка постачає систему ШІ, засоби, послуги, компоненти або процеси, що використовуються або інтегровані у висококризиковану систему ШІ, письмовою угодою визначають необхідну інформацію, можливості, технічний доступ та іншу підтримку на основі загальновизнаного стану мистецтва, щоб дати змогу постачальнику висококризикованої системи ШІ повністю виконати зобов'язання, встановлені у цьому Регламенті. Цей параграф не застосовується до третіх сторін, що забезпечують публічний доступ до засобів, послуг, процесів або компонентів, крім загальноцільових моделей ШІ, за вільною ліцензією з відкритим вихідним кодом.

Офіс ШІ може розробляти та рекомендувати добровільні модельні умови для контрактів між постачальниками висококризикованих систем ШІ та третіми сторонами, що постачають засоби, послуги, компоненти або процеси, що використовуються для висококризикованих систем ШІ або інтегровані в них. При розробці таких добровільних модельних умов Офіс ШІ враховує можливі договірні вимоги, що застосовуються в конкретних секторах або ділових випадках. Добровільні модельні умови публікуються та є доступними безкоштовно в легко використовуваному електронному форматі.

5. Параграфи 2 та 3 не завдають шкоди необхідності дотримання та захисту прав інтелектуальної власності, конфіденційної ділової інформації та комерційних таємниць відповідно до законодавства Союзу та національного законодавства.

Стаття 26

Зобов'язання суб'єктів розгортання високоризикованих систем ШІ

1. Суб'єкти розгортання високоризикованих систем ШІ вживають відповідних технічних та організаційних заходів для забезпечення використання таких систем відповідно до інструкцій з використання, що супроводжують системи, згідно з параграфами 3 і 6.

2. Суб'єкти розгортання призначають нагляд з боку людини фізичним особам, які мають необхідну компетентність, підготовку та повноваження, а також необхідну підтримку.

3. Зобов'язання, викладені в параграфах 1 і 2, не обмежують інших зобов'язань суб'єкта розгортання відповідно до права Союзу або національного права та свободи суб'єкта розгортання організовувати власні ресурси і діяльність з метою впровадження заходів нагляду з боку людини, зазначених постачальником.

4. Без обмеження параграфів 1 і 2, тією мірою, якою суб'єкт розгортання здійснює контроль над вхідними даними, такий суб'єкт розгортання забезпечує, щоб вхідні дані були відповідними та достатньо репрезентативними з огляду на передбачувану мету високоризикованої системи ШІ.

5. Суб'єкти розгортання здійснюють моніторинг роботи високоризикованої системи ШІ на основі інструкцій з використання і, де доречно, інформують постачальників відповідно до статті 72. Якщо суб'єкти розгортання мають підстави вважати, що використання високоризикованої системи ШІ відповідно до інструкцій може призвести до того, що ця система ШІ становитиме ризик у значенні статті 79(1), вони без невиправданої затримки інформують постачальника або дистриб'ютора та відповідний орган ринкового нагляду і зупиняють використання такої системи. Якщо суб'єкти розгортання виявили серйозний інцидент, вони також негайно інформують спочатку постачальника, а потім імпортера або дистриб'ютора та відповідні органи ринкового нагляду про такий інцидент. Якщо суб'єкт розгортання не може зв'язатися з постачальником, застосовується стаття 73 mutatis mutandis. Це зобов'язання не поширюється на чутливі оперативні дані суб'єктів розгортання систем ШІ, які є органами правоохоронної діяльності.

Для суб'єктів розгортання, які є фінансовими установами, що підпадають під вимоги щодо їхнього внутрішнього управління, заходів або процесів відповідно до права Союзу про фінансові послуги, зобов'язання щодо моніторингу, викладене в першому підпараграфі, вважається виконаним при дотриманні правил щодо заходів, процесів і механізмів внутрішнього управління відповідно до відповідного законодавства про фінансові послуги.

6. Суб'єкти розгортання високоризикованих систем ШІ зберігають журнали, автоматично генеровані такою високоризикованою системою ШІ, тією мірою, якою такі журнали перебувають під їхнім контролем, протягом відповідного призначеній меті високоризикованої системи ШІ періоду,

щонайменше шість місяців, якщо інше не передбачено застосовним правом Союзу або національним правом, зокрема правом Союзу про захист персональних даних.

Суб'єкти розгортання, які є фінансовими установами, що підпадають під вимоги щодо їхнього внутрішнього управління, заходів або процесів відповідно до права Союзу про фінансові послуги, зберігають журнали як частину документації, що ведеться відповідно до відповідного права Союзу про фінансові послуги.

7. До введення в експлуатацію або використання високоризикованої системи ШІ на робочому місці суб'єкти розгортання, які є роботодавцями, інформують представників працівників і відповідних працівників про те, що вони будуть підлягати використанню високоризикованої системи ШІ. Ця інформація надається, де застосовно, відповідно до правил і процедур, встановлених у праві та практиці Союзу і національному праві щодо інформування працівників та їхніх представників.

8. Суб'єкти розгортання високоризикованих систем ШІ, які є органами публічної влади, або установами, органами, офісами чи агентствами Союзу, дотримуються зобов'язань щодо реєстрації, зазначених у статті 49. Якщо такі суб'єкти розгортання виявляють, що високоризикована система ШІ, яку вони планують використовувати, не зареєстрована в базі даних ЄС, зазначеній у статті 71, вони не використовують таку систему і інформують постачальника або дистриб'ютора.

9. Де застосовно, суб'єкти розгортання високоризикованих систем ШІ використовують інформацію, надану відповідно до статті 13 цього Регламенту, для виконання свого зобов'язання щодо проведення оцінки впливу на захист даних відповідно до статті 35 Регламенту (ЄС) 2016/679 або статті 27 Директиви (ЄС) 2016/680.

10. Без обмеження Директиви (ЄС) 2016/680, у рамках розслідування для цільового пошуку особи, підозрюваної або засудженої за вчинення кримінального правопорушення, суб'єкт розгортання високоризикованої системи ШІ для постфактичної дистанційної біометричної ідентифікації запитує дозвіл, ex ante, або без невиправданої затримки і не пізніше ніж через 48 годин, від судового органу або адміністративного органу, рішення якого є обов'язковим і підлягає судовому перегляду, для використання такої системи, крім випадків, коли вона використовується для початкової ідентифікації потенційного підозрюваного на основі об'єктивних і перевірених фактів, безпосередньо пов'язаних із правопорушенням. Кожне використання обмежується тим, що суворо необхідно для розслідування конкретного кримінального правопорушення.

Якщо дозвіл, запитаний відповідно до першого підпараграфу, відхилено, використання системи постфактичної дистанційної біометричної ідентифікації, пов'язаної з таким запитаним дозволом, негайно зупиняється, а персональні дані, пов'язані з використанням високоризикованої системи ШІ, для якої було запитано дозвіл, видаляються.

У жодному разі така високоризикована система ШІ для постфактичної дистанційної біометричної ідентифікації не може використовуватися з метою правоохоронної діяльності нецільовим чином, без будь-якого зв'язку з кримінальним правопорушенням, кримінальним провадженням, реальною та наявною або реальною та передбачуваною загрозою кримінального правопорушення, або з пошуком конкретної зниклої особи. Забезпечується, щоб жодне рішення, що тягне несприятливі правові наслідки для особи, не могло бути прийняте правоохоронними органами виключно на основі виходу таких систем постфактичної дистанційної біометричної ідентифікації.

Цей параграф не обмежує статтю 9 Регламенту (ЄС) 2016/679 та статтю 10 Директиви (ЄС) 2016/680 щодо обробки біометричних даних.

Незалежно від мети або суб'єкта розгортання, кожне використання таких високоризикованих систем ШІ документується у відповідному поліцейському файлі і надається відповідному органу ринкового нагляду та національному органу із захисту даних на запит, за винятком розкриття чутливих оперативних даних, пов'язаних із правоохоронною діяльністю. Цей підпараграф не обмежує повноваження, надані Директивою (ЄС) 2016/680 наглядовим органам.

Суб'єкти розгортання подають щорічні звіти до відповідних органів ринкового нагляду та національних органів із захисту даних щодо їхнього використання систем постфактичної дистанційної біометричної ідентифікації, за винятком розкриття чутливих оперативних даних, пов'язаних із правоохоронною діяльністю. Звіти можуть бути агреговані для охоплення більш ніж одного розгортання.

Держави-члени можуть запроваджувати, відповідно до права Союзу, більш обмежувальне законодавство щодо використання систем постфактичної дистанційної біометричної ідентифікації.

11. Без обмеження статті 50 цього Регламенту, суб'єкти розгортання високоризикованих систем ШІ, зазначених у Додатку III, які приймають рішення або допомагають у прийнятті рішень, що стосуються фізичних осіб, інформують фізичних осіб про те, що вони є суб'єктами використання високоризикованої системи ШІ. Для високоризикованих систем ШІ, що використовуються з метою правоохоронної діяльності, застосовується стаття 13 Директиви (ЄС) 2016/680.

12. Суб'єкти розгортання співпрацюють з відповідними компетентними органами в будь-яких діях, які ці органи вживають щодо високоризикованої системи ШІ з метою виконання цього Регламенту.

Стаття 27

Оцінка впливу на основні права для високоризикованих систем ШІ

1. До розгортання високоризикованої системи ШІ, зазначеної в статті 6(2), за винятком високоризикованих систем ШІ, призначених для використання у сфері, зазначеній у пункті 2 Додатка III, суб'єкти розгортання, які є органами, що управляються публічним правом, або є приватними суб'єктами, що надають публічні послуги, та суб'єкти розгортання високоризикованих систем ШІ, зазначених у пунктах 5(b) та (c) Додатка III, проводять оцінку впливу на основні права, який може спричинити використання такої системи. З цією метою суб'єкти розгортання проводять оцінку, що складається з:

(a) опису процесів суб'єкта розгортання, в яких буде використовуватися високоризикована система ШІ відповідно до її призначеної мети;

(b) опису часового проміжку, протягом якого, та частоти, з якою кожна високоризикована система ШІ призначена для використання;

(c) категорій фізичних осіб і груп, на які, ймовірно, вплине її використання в конкретному контексті;

(d) конкретних ризиків заподіяння шкоди, які можуть вплинути на категорії фізичних осіб або груп осіб, визначених відповідно до пункту (c) цього параграфу, з урахуванням інформації, наданої постачальником відповідно до статті 13;

(e) опису впровадження заходів нагляду з боку людини відповідно до інструкцій з використання;

(f) заходів, що вживаються у разі реалізації таких ризиків, включаючи заходи щодо внутрішнього управління та механізми подання скарг.

2. Зобов'язання, викладене в параграфі 1, застосовується до першого використання високоризикованої системи ШІ. Суб'єкт розгортання може в аналогічних випадках спиратися на раніше проведені оцінки впливу на основні права або наявні оцінки впливу, проведені постачальником. Якщо під час використання високоризикованої системи ШІ суб'єкт розгортання вважає, що будь-який із елементів, перелічених у параграфі 1, змінився або більше не є актуальним, суб'єкт розгортання вживає необхідних кроків для оновлення інформації.

3. Після проведення оцінки, зазначеної в параграфі 1 цієї статті, суб'єкт розгортання повідомляє органу ринкового нагляду про її результати, подаючи заповнений шаблон, зазначений у параграфі 5 цієї статті, як частину повідомлення. У випадку, зазначеному в статті 46(1), суб'єкти розгортання можуть бути звільнені від цього зобов'язання щодо повідомлення.

4. Якщо будь-яке із зобов'язань, викладених у цій статті, вже виконане за допомогою оцінки впливу на захист даних, проведеної відповідно до статті 35 Регламенту (ЄС) 2016/679 або статті 27 Директиви (ЄС) 2016/680, оцінка впливу на основні права, зазначена в параграфі 1 цієї статті, доповнює таку оцінку впливу на захист даних.

5. Офіс ШІ розробляє шаблон анкети, включаючи через автоматизований інструмент, для сприяння суб'єктам розгортання у виконанні їхніх зобов'язань відповідно до цієї статті у спрощений спосіб.

РОЗДІЛ 4

Повідомні органи та нотифіковані органи

Стаття 28

Повідомляючі органи

1. Кожна держава-член призначає або засновує принаймні один повідомляючий орган, відповідальний за встановлення та здійснення необхідних процедур для оцінки, призначення та нотифікації органів оцінки відповідності та їхнього моніторингу. Ці процедури розробляються у співпраці між повідомляючими органами всіх держав-членів.

2. Держави-члени можуть вирішити, що оцінка та моніторинг, зазначені в параграфі 1, здійснюються національним органом з акредитації у значенні та відповідно до Регламенту (ЄС) № 765/2008.

3. Повідомляючі органи засновуються, організовуються та функціонують таким чином, щоб не виникало конфлікту інтересів з органами оцінки відповідності, а об'єктивність та неупередженість їхньої діяльності були захищені.

4. Повідомляючі органи організовуються таким чином, щоб рішення щодо нотифікації органів оцінки відповідності приймалися компетентними особами, відмінними від тих, хто проводив оцінку цих органів.

5. Повідомляючі органи не пропонують і не надають ні будь-яких видів діяльності, що виконуються органами оцінки відповідності, ні будь-яких консультаційних послуг на комерційній або конкурентній основі.

6. Повідомляючі органи забезпечують конфіденційність інформації, яку вони отримують, відповідно до статті 78.

7. Повідомляючі органи мають у своєму розпорядженні достатню кількість компетентного персоналу для належного виконання своїх завдань. Компетентний персонал повинен мати необхідну експертизу, де застосовно, для своєї функції, у таких сферах, як інформаційні технології, ШІ і право, включаючи нагляд за основними правами.

Стаття 29

Подання заяви органом оцінки відповідності для нотифікації

1. Органи оцінки відповідності подають заявку на нотифікацію до повідомляючого органу держави-члена, в якій вони засновані.

2. Заявка на нотифікацію супроводжується описом діяльності з оцінки відповідності, модулем або модулями оцінки відповідності та типами систем ШІ, щодо яких орган оцінки відповідності заявляє про свою компетентність, а також сертифікатом акредитації, якщо такий існує, виданим національним органом з акредитації, що підтверджує відповідність органу оцінки відповідності вимогам, викладеним у статті 31.

Будь-який дійсний документ, пов'язаний з наявними призначеннями нотифікованого органу-заявника відповідно до будь-якого іншого законодавства Союзу про гармонізацію, додається.

3. Якщо відповідний орган оцінки відповідності не може надати сертифікат акредитації, він надає повідомляючому органу всі документальні докази, необхідні для перевірки, визнання та регулярного моніторингу його відповідності вимогам, викладеним у статті 31.

4. Для нотифікованих органів, призначених відповідно до будь-якого іншого законодавства Союзу про гармонізацію, усі документи та сертифікати, пов'язані з такими призначеннями, можуть використовуватися для підтримки їхньої процедури призначення відповідно до цього Регламенту, де доречно. Нотифікований орган оновлює документацію, зазначену в параграфах 2 і 3 цієї статті, щоразу коли відбуваються відповідні зміни, щоб дати змогу органу, відповідальному за нотифіковані органи, здійснювати моніторинг і перевіряти постійну відповідність усім вимогам, викладеним у статті 31.

Стаття 30

Процедура нотифікації

1. Повідомляючі органи можуть нотифікувати лише органи оцінки відповідності, які задовольнили вимоги, викладені в статті 31.

2. Повідомляючі органи повідомляють Комісію та інші держави-члени, використовуючи електронний інструмент нотифікації, розроблений та керований Комісією, про кожен орган оцінки відповідності, зазначений у параграфі 1.

3. Нотифікація, зазначена в параграфі 2 цієї статті, включає повні відомості про діяльність з оцінки відповідності, модуль або модулі оцінки відповідності, типи відповідних систем ШІ та відповідне свідоцтво про компетентність. Якщо нотифікація не ґрунтується на сертифікаті акредитації, як зазначено в статті 29(2), повідомляючий орган надає Комісії та іншим державам-членам документальні докази, що підтверджують компетентність органу оцінки відповідності та заходи, що забезпечують регулярний моніторинг цього органу і подальше задоволення ним вимог, викладених у статті 31.

4. Відповідний орган оцінки відповідності може виконувати діяльність нотифікованого органу лише за умови, що Комісія або інші держави-члени не висловлюють заперечень протягом двох тижнів від нотифікації повідомляючим органом, якщо вона включає сертифікат акредитації, зазначений у статті 29(2), або протягом двох місяців від нотифікації повідомляючим органом, якщо вона включає документальні докази, зазначені в статті 29(3).

5. Якщо висловлено заперечення, Комісія без затримки вступає в консультації з відповідними державами-членами та органом оцінки відповідності. З огляду на це Комісія вирішує, чи є авторизація обґрунтованою. Комісія направляє своє рішення відповідній державі-члену та відповідному органу оцінки відповідності.

Стаття 31

Вимоги до нотифікованих органів

1. Нотифікований орган засновується відповідно до національного законодавства держави-члена та має статус юридичної особи.

2. Нотифіковані органи відповідають організаційним вимогам, вимогам до управління якістю, ресурсів та процесів, необхідних для виконання їхніх завдань, а також відповідним вимогам кібербезпеки.

3. Організаційна структура, розподіл відповідальності, підзвітність та функціонування нотифікованих органів забезпечують впевненість у їхній діяльності та у результатах діяльності з оцінки відповідності, яку здійснюють нотифіковані органи.

4. Нотифіковані органи є незалежними від постачальника висококризискованої системи ШІ, щодо якої вони здійснюють діяльність з оцінки відповідності. Нотифіковані органи також є незалежними від будь-якого іншого оператора, що має економічний інтерес у оцінюваних висококризискованих системах ШІ, а також від будь-яких конкурентів постачальника. Це не перешкоджає використанню оцінених висококризискованих систем ШІ, необхідних для діяльності органу оцінки відповідності, або використанню таких висококризискованих систем ШІ в особистих цілях.

5. Ні орган оцінки відповідності, ні його вище керівництво, ні персонал, відповідальний за виконання завдань з оцінки відповідності, не беруть безпосередньої участі у проектуванні, розробці, маркетингу або використанні висококризискованих систем ШІ, а також не представляють сторін, що беруть участь у зазначеній діяльності. Вони не беруть участі в жодній діяльності, яка може суперечити їхній незалежності судження або доброчесності щодо діяльності з оцінки відповідності, стосовно якої вони нотифіковані. Це стосується, зокрема, консультаційних послуг.

6. Нотифіковані органи організовуються та функціонують таким чином, щоб забезпечити незалежність, об'єктивність та неупередженість їхньої діяльності. Нотифіковані органи документують та впроваджують структуру і процедури для забезпечення неупередженості та поширення і застосування принципів неупередженості в межах своєї організації, персоналу та діяльності з оцінки.

7. Нотифіковані органи мають задокументовані процедури, що забезпечують дотримання їхнім персоналом, комітетами, дочірніми підприємствами, субпідрядниками та будь-яким асоційованим органом або персоналом зовнішніх органів, відповідно до статті 78, конфіденційності інформації, що надходить до їхнього розпорядження під час здійснення діяльності з оцінки відповідності, крім випадків, коли її розкриття вимагається законом. Персонал нотифікованих органів зобов'язаний дотримуватися професійної таємниці щодо всієї інформації, отриманої під час виконання своїх завдань відповідно до цього Регламенту, крім випадків, що стосуються повідомляючих органів держави-члена, в якій здійснюється їхня діяльність.

8. Нотифіковані органи мають процедури для здійснення діяльності, які належним чином враховують розмір постачальника, сектор, в якому він діє, його структуру та ступінь складності відповідної системи ШІ.

9. Нотифіковані органи укладають відповідне страхування відповідальності для своєї діяльності з оцінки відповідності, якщо тільки відповідальність не бере на себе держава-член, в якій вони засновані, відповідно до національного законодавства, або якщо така держава-член сама безпосередньо несе відповідальність за оцінку відповідності.

10. Нотифіковані органи здатні виконувати всі свої завдання відповідно до цього Регламенту з найвищим ступенем професійної доброчесності та необхідною компетентністю у відповідній сфері, незалежно від того, чи виконуються ці завдання самими нотифікованими органами, чи від їхнього імені та під їхньою відповідальністю.

11. Нотифіковані органи мають достатні внутрішні компетенції для ефективного оцінювання завдань, що виконуються зовнішніми сторонами від їхнього імені. Нотифікований орган забезпечує постійну наявність достатнього адміністративного, технічного, юридичного та наукового персоналу, який має досвід і знання стосовно відповідних типів систем ШІ, даних та обчислення даних, а також щодо вимог, викладених у розділі 2.

12. Нотифіковані органи беруть участь у координаційних заходах, зазначених у статті 38. Вони також безпосередньо беруть участь або представлені в європейських організаціях зі стандартизації, або забезпечують поінформованість та актуальність своїх знань щодо відповідних стандартів.

Стаття 32

Презумпція відповідності вимогам щодо нотифікованих органів

Якщо орган оцінки відповідності демонструє свою відповідність критеріям, викладеним у відповідних гармонізованих стандартах або їхніх частинах, посилання на які було опубліковано в Офіційний журнал Європейського Союзу, вважається, що він відповідає вимогам, викладеним у статті 31, тією мірою, якою застосовні гармонізовані стандарти охоплюють ці вимоги.

Стаття 33

Дочірні підприємства нотифікованих органів та субпідряд

1. Якщо нотифікований орган передає на субпідряд конкретні завдання, пов'язані з оцінкою відповідності, або звертається до дочірнього підприємства, він забезпечує відповідність субпідрядника або дочірнього підприємства вимогам, викладеним у статті 31, та відповідно інформує повідомляючий орган.

2. Нотифіковані органи несуть повну відповідальність за завдання, що виконуються будь-якими субпідрядниками або дочірніми підприємствами.

3. Діяльність може передаватися на субпідряд або здійснюватися дочірнім підприємством лише за згодою постачальника. Нотифіковані органи оприлюднюють перелік своїх дочірніх підприємств.

4. Відповідні документи щодо оцінки кваліфікації субпідрядника або дочірнього підприємства та роботи, виконаної ними відповідно до цього Регламенту, зберігаються у розпорядженні повідомляючого органу протягом п'яти років від дати припинення субпідряду.

Стаття 34

Операційні зобов'язання нотифікованих органів

1. Нотифіковані органи перевіряють відповідність висококризискованих систем ШІ відповідно до процедур оцінки відповідності, викладених у статті 43.

2. Нотифіковані органи уникають зайвого навантаження на постачальників під час здійснення своєї діяльності та належним чином враховують розмір постачальника, сектор, в якому він діє, його структуру та ступінь складності відповідної висококризискованої системи ШІ, зокрема з метою мінімізації адміністративного навантаження та витрат на дотримання вимог для мікро- та малих підприємств у розумінні Рекомендації 2003/361/ЄС. Нотифікований орган, тим не менш, дотримується ступеня суворості та рівня захисту, необхідних для відповідності висококризискованої системи ШІ вимогам цього Регламенту.

3. Нотифіковані органи надають та подають на запит усю відповідну документацію, включаючи документацію постачальників, повідомляючому органу, зазначеному у статті 28, щоб дозволити цьому органу здійснювати свою діяльність з оцінки, призначення, нотифікації та моніторингу, а також для сприяння оцінці, окресленій у цьому розділі.

Стаття 35

Ідентифікаційні номери та переліки нотифікованих органів

1. Комісія присвоює єдиний ідентифікаційний номер кожному нотифікованому органу, навіть якщо орган нотифікований відповідно до більш ніж одного акта Союзу.

2. Комісія оприлюднює перелік органів, нотифікованих відповідно до цього Регламенту, включаючи їхні ідентифікаційні номери та види діяльності, стосовно яких вони були нотифіковані. Комісія забезпечує актуальність переліку.

Стаття 36

Зміни до нотифікацій

1. Повідомляючий орган повідомляє Комісію та інші держави-члени про будь-які відповідні зміни до нотифікації нотифікованого органу за допомогою електронного інструменту нотифікації, зазначеного у статті 30(2).

2. Процедури, викладені у статтях 29 і 30, застосовуються до розширення сфери дії нотифікації.

Щодо змін до нотифікації, які не є розширенням її сфери дії, застосовуються процедури, викладені в пунктах (3)–(9).

3. Якщо нотифікований орган вирішує припинити свою діяльність з оцінки відповідності, він якомога швидше інформує про це повідомний орган та відповідних постачальників і, у разі запланованого припинення, — принаймні за один рік до припинення своєї діяльності. Сертифікати нотифікованого органу можуть залишатися дійсними протягом дев'яти місяців після припинення діяльності нотифікованого органу за умови, що інший нотифікований орган підтвердив у письмовій формі, що він прийме на себе відповідальність за високоризикові системи штучного інтелекту, охоплені цими сертифікатами. Останній нотифікований орган завершує повну оцінку відповідних високоризикових систем штучного інтелекту до кінця цього дев'ятимісячного строку, перш ніж видати нові сертифікати для цих систем. Якщо нотифікований орган припинив свою діяльність, повідомний орган відкликає призначення.

4. Якщо повідомний орган має достатні підстави вважати, що нотифікований орган більше не відповідає вимогам, викладеним у статті 31, або що він не виконує свої зобов'язання, повідомний орган негайно розслідує цю справу з максимальною ретельністю. У цьому контексті він інформує відповідний нотифікований орган про висунуті заперечення та надає йому можливість висловити свою позицію. Якщо повідомний орган доходить висновку, що нотифікований орган більше не відповідає вимогам, викладеним у статті 31, або що він не виконує свої зобов'язання, він обмежує, призупиняє або відкликає призначення, залежно від серйозності невиконання цих вимог або зобов'язань. Він негайно відповідно інформує Комісію та інші держави-члени.

5. Якщо призначення нотифікованого органу було призупинено, обмежено або повністю чи частково відкликано, він інформує відповідних постачальників протягом 10 днів.

6. У разі обмеження, призупинення або відкликання призначення повідомний орган вживає відповідних заходів для забезпечення зберігання файлів відповідного нотифікованого органу та надання їх на запит повідомним органам в інших державах-членах та органам ринкового нагляду.

7. У разі обмеження, призупинення або відкликання призначення повідомний орган:

(а) оцінює вплив на сертифікати, видані нотифікованим органом;

(б) подає звіт про свої висновки до Комісії та інших держав-членів протягом трьох місяців після повідомлення про зміни у призначенні;

(в) вимагає від нотифікованого органу призупинити або відкликати протягом розумного строку, визначеного органом, будь-які сертифікати, які були видані неналежним чином, щоб забезпечити постійну відповідність високоризикових систем штучного інтелекту на ринку;

(г) інформує Комісію та держави-члени про сертифікати, призупинення або відкликання яких воно вимагало;

(д) надає національним компетентним органам держави-члена, в якій постачальник має своє зареєстроване місце провадження господарської діяльності, всю відповідну інформацію про сертифікати, призупинення або відкликання яких воно вимагало; цей орган вживає відповідних заходів, де це необхідно, щоб уникнути потенційного ризику для здоров'я, безпеки або основоположних прав.

8. За винятком неналежно виданих сертифікатів, якщо призначення було призупинено або обмежено, сертифікати залишаються дійсними за однієї з таких обставин:

(а) повідомний орган підтвердив протягом одного місяця після призупинення або обмеження, що немає жодного ризику для здоров'я, безпеки або основоположних прав щодо сертифікатів, на які поширюється призупинення або обмеження, і повідомний орган окреслив часові рамки для дій щодо усунення призупинення або обмеження; або

(б) повідомний орган підтвердив, що жодні сертифікати, пов'язані із призупиненням, не будуть видані, змінені або повторно видані протягом дії призупинення або обмеження, та зазначає, чи має нотифікований орган можливість продовжувати здійснювати моніторинг і залишатися відповідальним за наявні сертифікати, видані на строк призупинення або обмеження; у випадку, якщо повідомний орган визначає, що нотифікований орган не має можливості підтримувати наявні видані сертифікати, постачальник системи, охопленої сертифікатом, підтверджує в письмовій формі національним компетентним органам держави-члена, в якій він має своє

зареєстроване місце провадження господарської діяльності, протягом трьох місяців після призупинення або обмеження, що інший кваліфікований нотифікований орган тимчасово виконує функції нотифікованого органу з моніторингу і залишається відповідальним за сертифікати протягом строку призупинення або обмеження.

9. За винятком неналежно виданих сертифікатів, якщо призначення було відкликано, сертифікати залишаються дійсними протягом дев'яти місяців за таких обставин:

(а) національний компетентний орган держави-члена, в якій постачальник відповідної високоризикової системи штучного інтелекту, охопленої сертифікатом, має своє зареєстроване місце провадження господарської діяльності, підтвердив, що немає жодного ризику для здоров'я, безпеки або основоположних прав, пов'язаного з відповідними високоризиковими системами штучного інтелекту; та

(б) інший нотифікований орган підтвердив у письмовій формі, що він негайно бере на себе відповідальність за ці системи штучного інтелекту та завершує свою оцінку протягом 12 місяців після відкликання призначення.

За обставин, зазначених у першому підпункті, національний компетентний орган держави-члена, в якій постачальник системи, охопленої сертифікатом, має своє місце провадження господарської діяльності, може продовжити попередню дійсність сертифікатів на додаткові тримісячні строки, які в сукупності не повинні перевищувати 12 місяців.

Національний компетентний орган або нотифікований орган, що бере на себе функції нотифікованого органу, якого торкнулася зміна призначення, негайно інформує про це Комісію, інші держави-члени та інші нотифіковані органи.

Стаття 37

Оскарження компетентності нотифікованих органів

1. Комісія за необхідності розслідує всі випадки, коли є підстави сумніватися в компетентності нотифікованого органу або в постійному виконанні нотифікованим органом вимог, викладених у статті 31, та його застосовних обов'язків.

2. Повідомляючий орган надає Комісії на запит всю відповідну інформацію щодо нотифікації або підтримання компетентності відповідного нотифікованого органу.

3. Комісія забезпечує, щоб уся конфіденційна інформація, отримана в ході її розслідувань відповідно до цієї статті, оброблялася конфіденційно відповідно до статті 78.

4. Якщо Комісія встановлює, що нотифікований орган не відповідає або більше не відповідає вимогам для його нотифікації, вона відповідно інформує повідомляючу державу-член та просить вжити необхідних коригувальних заходів, включаючи призупинення або відкликання нотифікації, якщо це необхідно. Якщо держава-член не вживає необхідних коригувальних заходів, Комісія може за допомогою імплементаційного акта призупинити, обмежити або відкликати призначення. Цей імплементаційний акт ухвалюється відповідно до процедури розгляду, зазначеної в статті 98(2).

Стаття 38

Координація нотифікованих органів

1. Комісія забезпечує, щоб стосовно висококризикових систем ШІ належна координація та співпраця між нотифікованими органами, що беруть участь у процедурах оцінки відповідності відповідно до цього Регламенту, були запроваджені та належним чином функціонували у формі галузевої групи нотифікованих органів.

2. Кожен повідомляючий орган забезпечує участь нотифікованих ним органів у роботі групи, зазначеної в пункті 1, безпосередньо або через призначених представників.

3. Комісія забезпечує обмін знаннями та передовим досвідом між повідомляючими органами.

Стаття 39

Органи оцінки відповідності третіх країн

Органи оцінки відповідності, засновані відповідно до законодавства третьої країни, з якою Союз уклав угоду, можуть бути уповноважені здійснювати діяльність нотифікованих органів відповідно до цього Регламенту за умови, що вони відповідають вимогам, викладеним у статті 31, або забезпечують еквівалентний рівень відповідності.

РОЗДІЛ 5

Стандарти, оцінка відповідності, сертифікати, реєстрація

Стаття 40

Гармонізовані стандарти та результати стандартизації

1. Висококризикові системи ШІ або моделі ШІ загального призначення, які відповідають гармонізованим стандартам або їх частинам, посилання на які опубліковані в Офіційний журнал Європейського Союзу відповідно до Регламенту (ЄС) № 1025/2012, вважаються такими, що відповідають вимогам, викладеним у Розділі 2 цієї Глави, або, за необхідності, зобов'язанням, викладеним у Главі V, Розділах 2 і 3, цього Регламенту, тією мірою, якою такі стандарти охоплюють такі вимоги або зобов'язання.

2. Відповідно до статті 10 Регламенту (ЄС) № 1025/2012 Комісія без зайвого зволікання видає запити на стандартизацію, що охоплюють усі вимоги, встановлені в розділі 2 цієї глави, і, де це застосовно, запити на стандартизацію, що охоплюють зобов'язання, встановлені в главі V, розділах 2 та 3, цього Регламенту. Запит на стандартизацію також має передбачати результати щодо процесів звітування та документування для покращення ресурсних показників систем штучного інтелекту, наприклад, зменшення споживання енергії та інших ресурсів високоризиковою системою штучного інтелекту протягом її життєвого циклу, а також щодо енергоефективного розроблення моделей штучного інтелекту загального призначення. При підготовці запиту на стандартизацію Комісія консультується з Радою та відповідними зацікавленими сторонами, включаючи консультативний форум.

При направленні запиту на стандартизацію до європейських організацій зі стандартизації Комісія зазначає, що стандарти мають бути чіткими, узгодженими, у тому числі зі стандартами, розробленими в різних секторах для продуктів, охоплених чинним законодавством Союзу про гармонізацію, переліченим у Додатку I, і спрямованими на забезпечення того, що високоризикові системи штучного інтелекту або моделі штучного інтелекту загального призначення, виведені на ринок або введені в експлуатацію в Союзі, відповідають відповідним вимогам або зобов'язанням, встановленим у цьому Регламенті.

Комісія просить європейські організації зі стандартизації надати докази своїх максимальних зусиль щодо досягнення цілей, зазначених у першому та другому підпунктах цього пункту, відповідно до статті 24 Регламенту (ЄС) № 1025/2012.

3. Учасники процесу стандартизації прагнуть сприяти інвестиціям та інноваціям у сфері ШІ, зокрема шляхом підвищення правової визначеності, а також конкурентоспроможності та зростання ринку Союзу, сприяти зміцненню глобального співробітництва в галузі стандартизації та враховувати існуючі міжнародні стандарти у сфері ШІ, що відповідають цінностям, основоположним правам та інтересам Союзу, а також вдосконалювати управління за участю багатьох зацікавлених сторін, що забезпечує збалансоване представництво інтересів та ефективну участь усіх відповідних зацікавлених сторін відповідно до статей 5, 6 і 7 Регламенту (ЄС) № 1025/2012.

Стаття 41

Загальні специфікації

1. Комісія може ухвалювати імплементаційні акти, що встановлюють загальні специфікації для вимог, викладених у розділі 2 цієї глави, або, де це застосовно, для зобов'язань, викладених у розділах 2 та 3 глави V, за умови виконання таких умов:

(а) Комісія звернулася відповідно до статті 10(1) Регламенту (ЄС) № 1025/2012 до однієї чи кількох європейських організацій зі стандартизації з проханням розробити гармонізований стандарт для вимог, викладених у розділі 2 цієї глави, або, де це застосовно, для зобов'язань, викладених у розділах 2 та 3 глави V, і:

(i) запит не був прийнятий жодною з європейських організацій зі стандартизації; або

(ii) гармонізовані стандарти, що стосуються цього запиту, не надаються в строк, встановлений відповідно до статті 10(1) Регламенту (ЄС) № 1025/2012; або

(iii) відповідні гармонізовані стандарти недостатньо вирішують питання основоположних прав; або

(iv) гармонізовані стандарти не відповідають запиту; та

(б) жодне посилання на гармонізовані стандарти, що охоплюють вимоги, зазначені в розділі 2 цієї глави, або, де це застосовно, зобов'язання, зазначені в розділах 2 та 3 глави V, не було опубліковано в Офіційному журналі Європейського Союзу відповідно до Регламенту (ЄС) № 1025/2012, і жодного такого посилання не очікується до публікації в розумний строк.

При розробці загальних специфікацій Комісія консультується з консультативним форумом, зазначеним у статті 67.

Імплементаційні акти, зазначені в першому підпункті цього пункту, ухвалюються відповідно до процедури розгляду, зазначеної в статті 98(2).

2. Перед підготовкою проєкту імплементаційного акта Комісія інформує комітет, зазначений у статті 22 Регламенту (ЄС) № 1025/2012, про те, що вона вважає умови, викладені в пункті 1 цієї статті, виконаними.

3. Вважається, що високоризикові системи штучного інтелекту або моделі штучного інтелекту загального призначення, які відповідають загальним специфікаціям, зазначеним у пункті 1, або частинам цих специфікацій, відповідають вимогам, встановленим у розділі 2 цієї глави, або, де це застосовно, дотримуються зобов'язань, зазначених у розділах 2 та 3 глави V, тією мірою, якою ці загальні специфікації охоплюють ці вимоги або ці зобов'язання.

4. Якщо гармонізований стандарт прийнятий європейською організацією зі стандартизації та запропонований Комісії для публікації посилання на нього в Офіційному журналі Європейського Союзу, Комісія оцінює гармонізований стандарт відповідно до Регламенту (ЄС) № 1025/2012. Коли посилання на гармонізований стандарт публікується в Офіційному журналі Європейського Союзу, Комісія скасовує імплементаційні акти, зазначені в пункті 1, або їхні частини, що охоплюють ті самі вимоги, встановлені в розділі 2 цієї глави, або, де це застосовно, ті самі зобов'язання, встановлені в розділах 2 та 3 глави V.

5. Якщо постачальники висококризикових систем ШІ або загальноцільових моделей ШІ не дотримуються загальних специфікацій, зазначених у параграфі 1, вони належним чином обґрунтовують, що вони прийняли технічні рішення, які відповідають вимогам, зазначеним у Розділі 2 цієї Глави, або, якщо застосовно, виконують зобов'язання, викладені у Розділах 2 і 3 Глави V, щонайменше на еквівалентному рівні.

6. Якщо держава-член вважає, що загальна специфікація не повністю відповідає вимогам, викладеним у Розділі 2, або, якщо застосовно, не виконує зобов'язань, викладених у Розділах 2 і 3 Глави V, вона інформує про це Комісію з детальним поясненням. Комісія оцінює цю інформацію і, якщо необхідно, вносить зміни до імплементаційного акта, що встановлює відповідну загальну специфікацію.

Стаття 42

Презумпція відповідності певним вимогам

1. Вважається, що висококризикові системи ШІ, які були навчені та протестовані на даних, що відображають конкретне географічне, поведінкове, контекстуальне або функціональне середовище, в якому вони призначені для використання, відповідають відповідним вимогам, викладеним у статті 10(4).

2. Вважається, що високоризикові системи штучного інтелекту, які були сертифіковані або для яких була видана заява про відповідність в рамках схеми кібербезпеки відповідно до Регламенту (ЄС) 2019/881 та посилання на які були опубліковані в Офіційному журналі Європейського Союзу , відповідають вимогам кібербезпеки, встановленим у статті 15 цього Регламенту, тією мірою, якою сертифікат кібербезпеки або заява про відповідність або їх частини охоплюють ці вимоги.

Стаття 43

Оцінка відповідності

1. Для висококризикованих систем ШІ, перелічених у пункті 1 Додатку III, де, при демонстрації відповідності висококризикованої системи ШІ вимогам, викладеним у Розділі 2, постачальник застосував гармонізовані стандарти, зазначені у статті 40, або, де це застосовно, загальні

специфікації, зазначені у статті 41, постачальник обирає одну з таких процедур оцінки відповідності на основі:

(a) внутрішнього контролю, зазначеного в Додатку VI; або

(b) оцінки системи управління якістю та оцінки технічної документації за участю нотифікованого органу, зазначених у Додатку VII.

При демонстрації відповідності висококризикованої системи ШІ вимогам, викладеним у Розділі 2, постачальник дотримується процедури оцінки відповідності, встановленої у Додатку VII, де:

(a) гармонізовані стандарти, зазначені у статті 40, не існують, і загальні специфікації, зазначені у статті 41, недоступні;

(b) постачальник не застосував або застосував лише частину гармонізованого стандарту;

(c) загальні специфікації, зазначені у пункті (a), існують, але постачальник не застосував їх;

(d) один або кілька гармонізованих стандартів, зазначених у пункті (a), були опубліковані з обмеженням, і лише щодо тієї частини стандарту, яка була обмежена.

Для цілей процедури оцінки відповідності, зазначеної у Додатку VII, постачальник може обрати будь-який з нотифікованих органів. Однак, якщо висококризикована система ШІ призначена для введення в експлуатацію правоохоронними, міграційними або органами з питань притулку або інститутами, органами, установами чи агентствами Союзу, орган ринкового нагляду, зазначений у статті 74(8) або (9), залежно від обставин, діє як нотифікований орган.

2. Для висококризикованих систем ШІ, зазначених у пунктах 2–8 Додатку III, постачальники дотримуються процедури оцінки відповідності на основі внутрішнього контролю, зазначеної у Додатку VI, яка не передбачає участі нотифікованого органу.

3. Для висококризикованих систем ШІ, охоплених гармонізаційним законодавством Союзу, переліченим у Розділі A Додатку I, постачальник дотримується відповідної процедури оцінки відповідності, що вимагається відповідно до таких правових актів. Вимоги, викладені у Розділі 2 цієї Глави, застосовуються до таких висококризикованих систем ШІ і є частиною такої оцінки. Пункти 4.3., 4.4., 4.5. та п'ятий підпараграф пункту 4.6 Додатку VII також застосовуються.

Для цілей такої оцінки нотифіковані органи, що були нотифіковані відповідно до таких правових актів, мають право контролювати відповідність висококризикованих систем ШІ вимогам, викладеним у Розділі 2, за умови, що відповідність таких нотифікованих органів вимогам, встановленим у статті 31(4), (5), (10) та (11), була оцінена в контексті процедури нотифікації відповідно до таких правових актів.

Якщо правовий акт, перелічений у Розділі А Додатку I, дає змогу виробнику продукту відмовитися від оцінки відповідності третьою стороною за умови, що такий виробник застосував всі гармонізовані стандарти, що охоплюють всі відповідні вимоги, такий виробник може скористатися цим варіантом лише у випадку, якщо він також застосував гармонізовані стандарти або, де це застосовно, загальні специфікації, зазначені у статті 41, що охоплюють всі вимоги, викладені у Розділі 2 цієї Глави.

4. Висококризиковані системи ШІ, що вже пройшли процедуру оцінки відповідності, проходять нову процедуру оцінки відповідності у разі суттєвої модифікації, незалежно від того, чи призначена модифікована система для подальшого розповсюдження або продовжує використовуватися поточним суб'єктом розгортання.

Для висококризикованих систем ШІ, що продовжують навчатися після розміщення на ринку або введення в експлуатацію, зміни до висококризикованої системи ШІ та її продуктивності, що були попередньо визначені постачальником на момент первинної оцінки відповідності та є частиною інформації, що міститься в технічній документації, зазначеній у пункті 2(f) Додатку IV, не становлять суттєвої модифікації.

5. Комісія уповноважена приймати делеговані акти відповідно до статті 97 для внесення змін до Додатків VI та VII шляхом їх оновлення з урахуванням технічного прогресу.

6. Комісія уповноважена приймати делеговані акти відповідно до статті 97 для внесення змін до параграфів 1 та 2 цієї статті з метою піддавання висококризикованих систем ШІ, зазначених у пунктах 2–8 Додатку III, процедурі оцінки відповідності, зазначеній у Додатку VII, або її частинам. Комісія приймає такі делеговані акти з урахуванням ефективності процедури оцінки відповідності на основі внутрішнього контролю, зазначеної у Додатку VI, у запобіганні або мінімізуванні ризиків для здоров'я та безпеки і захисту основних прав, що становлять такі системи, а також наявності достатніх потужностей та ресурсів серед нотифікованих органів.

Стаття 44

Сертифікати

1. Сертифікати, видані нотифікованими органами відповідно до Додатка VII, складаються мовою, яка може бути легко зрозумілою для відповідних органів держави-члена, в якій засновано нотифікований орган.

2. Сертифікати є чинними протягом терміну, який вони зазначають, що не може перевищувати п'ять років для систем ШІ, охоплених Додатком I, і чотири роки для систем ШІ, охоплених Додатком III. На запит постачальника термін дії сертифіката може бути продовжений на подальші терміни, кожен з яких не перевищує п'яти років для систем ШІ, охоплених Додатком I, і чотирьох років для систем ШІ, охоплених Додатком III, на основі повторної оцінки відповідно до застосовних процедур оцінки відповідності. Будь-яке доповнення до сертифіката залишається чинним за умови, що сертифікат, до якого воно є доповненням, є чинним.

3. Якщо нотифікований орган виявляє, що система ШІ більше не відповідає вимогам, викладеним у Розділі 2, він з урахуванням принципу пропорційності призупиняє або відкликає виданий сертифікат або накладає на нього обмеження, якщо дотримання цих вимог не забезпечено належними коригувальними діями, вжитими постачальником системи у відповідний строк, встановлений нотифікованим органом. Нотифікований орган надає обґрунтування свого рішення.

Має бути передбачена процедура оскарження рішень нотифікованих органів, у тому числі щодо виданих сертифікатів відповідності.

Стаття 45

Інформаційні зобов'язання нотифікованих органів

1. Нотифіковані органи інформують повідомний орган про таке:

(а) будь-які сертифікати оцінки технічної документації Союзу, будь-які доповнення до цих сертифікатів та будь-які схвалення системи управління якістю, видані відповідно до вимог Додатка VII;

(б) будь-яку відмову, обмеження, призупинення або відкликання сертифіката оцінки технічної документації Союзу або схвалення системи управління якістю, виданих відповідно до вимог Додатка VII;

(в) будь-які обставини, що впливають на сферу дії або умови нотифікації;

(г) будь-який запит на інформацію, який вони отримали від органів ринкового нагляду щодо діяльності з оцінки відповідності;

(д) на запит, діяльність з оцінки відповідності, здійснювану в межах їхньої нотифікації, та будь-яку іншу виконану діяльність, включаючи транскордонну діяльність та субпідряд.

2. Кожен нотифікований орган інформує інші нотифіковані органи про:

(а) схвалення системи управління якістю, у яких він відмовив, які призупинив або відкликав, а також на запит — про схвалення системи управління якістю, які він видав;

(б) сертифікати оцінки технічної документації Союзу або будь-які доповнення до них, у яких він відмовив, які відкликав, призупинив або іншим чином обмежив, а також на запит — про сертифікати та/або доповнення до них, які він видав.

3. Кожен нотифікований орган надає іншим нотифікованим органам, що здійснюють аналогічну діяльність з оцінки відповідності, що охоплює ті самі типи систем штучного інтелекту, відповідну інформацію з питань, що стосуються негативних та, на запит, позитивних результатів оцінки відповідності.

4. Нотифіковані органи забезпечують конфіденційність інформації, яку вони отримують, відповідно до статті 78.

Стаття 46

Відступ від процедури оцінки відповідності

1. У порядку відступу від статті 43 та на підставі належним чином обгрунтованого запиту будь-який орган ринкового нагляду може дозволити введення в обіг або введення в експлуатацію конкретних висококризикованих систем ШІ на території відповідної держави-члена з виняткових міркувань суспільної безпеки або захисту життя і здоров'я осіб, захисту довкілля або захисту ключових промислових та інфраструктурних об'єктів. Такий дозвіл видається на обмежений строк, протягом якого проводяться необхідні процедури оцінки відповідності, з урахуванням виняткових причин, що обгрунтовують відступ. Завершення цих процедур здійснюється без невиправданих зволікань.

2. У належним чином обгрунтованій ситуації нагальної необхідності з виняткових міркувань суспільної безпеки або у разі конкретної, істотної та невідворотної загрози життю чи фізичній безпеці фізичних осіб правоохоронні органи або органи цивільного захисту можуть ввести в експлуатацію конкретну висококризиковану систему ШІ без дозволу, зазначеного в параграфі 1, за умови що такий дозвіл запитується під час або після використання без невиправданих зволікань. Якщо у дозволі, зазначеному в параграфі 1, відмовлено, використання висококризикованої системи ШІ негайно припиняється, а всі результати та вихідні дані такого використання негайно знищуються.

3. Дозвіл, зазначений у параграфі 1, видається лише в тому разі, якщо орган ринкового нагляду доходить висновку, що висококризикована система ШІ відповідає вимогам розділу 2. Орган ринкового нагляду інформує Комісію та інші держави-члени про будь-який дозвіл, виданий відповідно до параграфів 1 і 2. Це зобов'язання не поширюється на чутливі оперативні дані, пов'язані з діяльністю правоохоронних органів.

4. Якщо протягом 15 календарних днів з моменту отримання інформації, зазначеної в параграфі 3, жодна держава-член або Комісія не висунули заперечень щодо дозволу, виданого органом ринкового нагляду держави-члена відповідно до параграфу 1, такий дозвіл вважається обгрунтованим.

5. Якщо протягом 15 календарних днів з моменту отримання повідомлення, зазначеного в параграфі 3, держава-член висуває заперечення проти дозволу, виданого органом ринкового нагляду іншої держави-члена, або якщо Комісія вважає дозвіл таким, що суперечить праву Союзу, або висновок держав-членів щодо відповідності системи, зазначений у параграфі 3, необгрунтованим, Комісія без зволікань розпочинає консультації з відповідною державою-членом. Відповідні оператори залучаються до консультацій та мають можливість висловити свої погляди. З урахуванням цього Комісія вирішує, чи є дозвіл обгрунтованим. Комісія адресує своє рішення відповідній державі-члену та відповідним операторам.

6. Якщо Комісія вважає дозвіл необгрунтованим, він відкликається органом ринкового нагляду відповідної держави-члена.

7. Для висококризикованих систем ШІ, пов'язаних з продуктами, що підпадають під законодавство Союзу про гармонізацію, перелічене в розділі А додатка I, застосовуються лише відступи від оцінки відповідності, встановлені в цьому законодавстві Союзу про гармонізацію.

Стаття 47

Декларація відповідності ЄС

1. Постачальник складає письмову декларацію відповідності ЄС у машиночитаній формі, підписану фізично або електронно, для кожної висококризикованої системи ШІ та зберігає її у розпорядженні національних компетентних органів протягом 10 років після введення висококризикованої системи

ШІ в обіг або введення в експлуатацію. Декларація відповідності ЄС ідентифікує висококризиковану систему ШІ, для якої її було складено. Копія декларації відповідності ЄС надається відповідним національним компетентним органам на запит.

2. У декларації відповідності ЄС зазначається, що відповідна висококризикована система ШІ відповідає вимогам, викладеним у розділі 2. Декларація відповідності ЄС містить інформацію, викладену в додатку V, і перекладається мовою, яка може бути легко зрозумілою для національних компетентних органів держав-членів, у яких висококризикова система ШІ вводиться в обіг або надається.

3. У тих випадках, коли на висококризикові системи ШІ поширюється інше законодавство Союзу про гармонізацію, яке також вимагає декларації відповідності ЄС, складається єдина декларація відповідності ЄС щодо всього права Союзу, що застосовується до висококризикованої системи ШІ. Декларація містить всю інформацію, необхідну для ідентифікації законодавства Союзу про гармонізацію, до якого вона відноситься.

4. Складаючи декларацію відповідності ЄС, постачальник бере на себе відповідальність за відповідність вимогам, викладеним у розділі 2. Постачальник підтримує декларацію відповідності ЄС в актуальному стані належним чином.

5. Комісія уповноважена ухвалювати делеговані акти відповідно до статті 97 з метою внесення змін до додатка V шляхом оновлення змісту декларації відповідності ЄС, викладеного в цьому додатку, з метою запровадження елементів, що стають необхідними у світлі технічного прогресу.

Стаття 48

Маркування CE

1. Маркування CE підпорядковується загальним принципам, викладеним у статті 30 Регламенту (ЄС) № 765/2008.

2. Для висококризикованих систем ШІ, що надаються в цифровій формі, використовується цифрове маркування CE, лише якщо до нього можна легко отримати доступ через інтерфейс, через який здійснюється доступ до цієї системи, або через легко доступний машиночитаний код чи інші електронні засоби.

3. Маркування CE наноситься видимим, розбірливим та незмивним чином для висококризикованих систем ШІ. Якщо це неможливо або недоцільно з огляду на характер висококризикованої системи ШІ, воно наноситься на упаковку або на супровідну документацію, залежно від обставин.

4. У відповідних випадках маркування CE супроводжується ідентифікаційним номером нотифікованого органу, відповідального за процедури оцінки відповідності, викладені в статті 43. Ідентифікаційний номер нотифікованого органу наноситься самим органом або, за його вказівками, постачальником чи уповноваженим представником постачальника. Ідентифікаційний номер також зазначається у будь-яких рекламних матеріалах, у яких зазначається, що висококризикована система ШІ відповідає вимогам для маркування CE.

5. У тих випадках, коли на висококризикові системи ШІ поширюється інше право Союзу, яке також передбачає нанесення маркування CE, маркування CE вказує на те, що висококризикова система ШІ також відповідає вимогам цього іншого права.

Стаття 49

Реєстрація

1. Перед введенням в обіг або введенням в експлуатацію висококризикованої системи ШІ, переліченої в додатку III, за винятком висококризикованих систем ШІ, зазначених у пункті 2 додатка III, постачальник або, у відповідних випадках, уповноважений представник реєструють себе та свою систему в базі даних ЄС, зазначеній у статті 71.

2. Перед введенням в обіг або введенням в експлуатацію системи ШІ, щодо якої постачальник дійшов висновку, що вона не є висококризиковою відповідно до статті 6(3), цей постачальник або, у відповідних випадках, уповноважений представник реєструють себе та цю систему в базі даних ЄС, зазначеній у статті 71.

3. Перед введенням в експлуатацію або використанням висококризикованої системи ШІ, переліченої в додатку III, за винятком висококризикованих систем ШІ, перелічених у пункті 2 додатка III, суб'єкти розгортання, що є органами публічної влади, установами, органами, службами або агентствами Союзу або особами, що діють від їхнього імені, реєструють себе, обирають систему та реєструють її використання в базі даних ЄС, зазначеній у статті 71.

4. Для високоризикових систем штучного інтелекту, зазначених у пунктах 1, 6 та 7 Додатка III, у сферах правоохоронної діяльності, міграції, притулку та управління прикордонним контролем, реєстрація, зазначена в пунктах 1, 2 та 3 цієї статті, здійснюється в захищеному непублічному розділі бази даних ЄС, зазначеній у статті 71, та включає лише таку інформацію, де це застосовно, зазначену в:

(а)	розділі A, пунктах 1–10 Додатка VIII, за винятком пунктів 6, 8 та 9;
(б)	розділі B, пунктах 1–5 та пунктах 8 та 9 Додатка VIII;
(в)	розділі C, пунктах 1–3 Додатка VIII;
(г)	пунктах 1, 2, 3 та 5 Додатка IX.

Лише Комісія та національні органи, зазначені в статті 74(8), матимуть доступ до відповідних обмежених розділів бази даних ЄС, перелічених у першому підпункті цього пункту.

5. Висококризикові системи ШІ, зазначені в пункті 2 додатка III, реєструються на національному рівні.

ГЛАВА IV

ЗОБОВ'ЯЗАННЯ ЩОДО ПРОЗОРОСТІ ДЛЯ ПОСТАЧАЛЬНИКІВ І СУБ'ЄКТІВ РОЗГОРТАННЯ ПЕВНИХ СИСТЕМ ШТУЧНОГО ІНТЕЛЕКТУ

Стаття 50

Зобов'язання щодо прозорості для постачальників та суб'єктів розгортання певних систем ШІ

1. Постачальники забезпечують, щоб системи ШІ, призначені для безпосередньої взаємодії з фізичними особами, проектувалися та розроблялися таким чином, щоб відповідні фізичні особи були поінформовані про те, що вони взаємодіють із системою ШІ, якщо тільки це не є очевидним з точки зору фізичної особи, яка є достатньо поінформованою, уважною та обачною, з урахуванням обставин та контексту використання. Це зобов'язання не застосовується до систем ШІ, уповноважених законом виявляти, запобігати, розслідувати або переслідувати за вчинення кримінальних правопорушень, за умови вжиття належних заходів захисту прав і свобод третіх осіб, якщо тільки ці системи не є доступними для громадськості з метою повідомлення про кримінальне правопорушення.

2. Постачальники систем ШІ, включаючи загальноцільові системи ШІ, що генерують синтетичний аудіо-, фото-, відео- або текстовий контент, забезпечують, щоб вихідні дані системи ШІ були позначені в машиночитаному форматі та могли бути виявлені як штучно згенеровані або маніпульовані. Постачальники забезпечують, щоб їхні технічні рішення були ефективними, сумісними, надійними та достовірними настільки, наскільки це технічно можливо, з урахуванням особливостей та обмежень різних типів контенту, витрат на впровадження та загальновизнаного рівня техніки, що може відображатися у відповідних технічних стандартах. Це зобов'язання не застосовується тією мірою, якою системи ШІ виконують допоміжну функцію для стандартного редагування або не змінюють суттєво вхідні дані, надані суб'єктом розгортання, або їх семантику, або у випадках, коли це дозволено законом для виявлення, запобігання, розслідування або переслідування кримінальних правопорушень.

3. Суб'єкти розгортання системи розпізнавання емоцій або системи біометричної категоризації інформують фізичних осіб, що зазнають впливу такої системи, про функціонування системи та обробляють персональні дані відповідно до Регламентів (ЄС) 2016/679 та (ЄС) 2018/1725 і Директиви (ЄС) 2016/680, залежно від обставин. Це зобов'язання не застосовується до систем ШІ, що використовуються для біометричної категоризації та розпізнавання емоцій, яким законом дозволено виявляти, запобігати або розслідувати кримінальні правопорушення, за умови вжиття належних заходів захисту прав і свобод третіх осіб та відповідно до права Союзу.

4. Суб'єкти розгортання системи ШІ, що генерує або маніпулює зображенням, аудіо- або відеоконтентом, що становить дипфейк, розкривають інформацію про те, що контент був штучно згенерований або маніпульований. Це зобов'язання не застосовується, якщо використання дозволено законом для виявлення, запобігання, розслідування або переслідування за вчинення кримінального правопорушення. Якщо контент є частиною явно художнього, творчого, сатиричного, художнього вигаданого або аналогічного твору чи програми, зобов'язання щодо прозорості, викладені в цьому параграфі, обмежуються розкриттям інформації про існування такого згенерованого або маніпульованого контенту в належний спосіб, що не перешкоджає показу або насолоді твором.

Суб'єкти розгортання системи ШІ, що генерує або маніпулює текстом, який публікується з метою інформування громадськості з питань суспільного інтересу, розкривають інформацію про те, що текст був штучно згенерований або маніпульований. Це зобов'язання не застосовується, якщо

використання дозволено законом для виявлення, запобігання, розслідування або переслідування за вчинення кримінальних правопорушень або якщо контент, згенерований ШІ, пройшов процес людської перевірки або редакційного контролю і якщо фізична або юридична особа несе редакційну відповідальність за публікацію контенту.

5. Інформація, зазначена в параграфах 1-4, надається відповідним фізичним особам у чіткий та виразний спосіб не пізніше ніж на момент першої взаємодії або впливу. Інформація відповідає застосовним вимогам доступності.

6. Параграфи 1-4 не впливають на вимоги та зобов'язання, викладені в главі III, і не обмежують інших зобов'язань щодо прозорості, встановлених у праві Союзу або національному праві для суб'єктів розгортання систем ШІ.

7. Офіс ШІ заохочує та сприяє розробці кодексів практики на рівні Союзу для сприяння ефективному виконанню зобов'язань щодо виявлення та маркування штучно згенерованого або маніпульованого контенту. Комісія може ухвалювати імплементаційні акти для затвердження цих кодексів практики відповідно до процедури, викладеної в статті 56(6). Якщо вона вважає кодекс неадекватним, Комісія може ухвалити імплементаційний акт, що визначає загальні правила виконання цих зобов'язань відповідно до процедури розгляду, викладеної в статті 98(2).

ГЛАВА V

МОДЕЛІ ШТУЧНОГО ІНТЕЛЕКТУ ЗАГАЛЬНОГО ПРИЗНАЧЕННЯ

РОЗДІЛ 1

Правила класифікації

Стаття 51

Класифікація загальноцільових моделей ШІ як загальноцільових моделей ШІ із системним ризиком

1. Загальноцільова модель ШІ класифікується як загальноцільова модель ШІ із системним ризиком, якщо вона відповідає будь-якій із таких умов:

(a) вона має можливості високого впливу, оцінені на основі відповідних технічних інструментів і методологій, включаючи показники та орієнтири;

(b) на підставі рішення Комісії, ex officio або за обґрунтованим сповіщенням наукового комітету, вона має можливості або вплив, еквівалентні тим, що визначені в пункті (a), з урахуванням критеріїв, викладених у Додатку XIII.

2. Вважається, що загальноцільова модель ШІ має можливості високого впливу відповідно до параграфа 1, пункту (a), коли сукупний обсяг обчислень, використаних для її навчання, виміряний у операціях з плаваючою комою, перевищує 1025.

3. Комісія приймає делеговані акти відповідно до Статті 97 для внесення змін до порогових значень, зазначених у параграфах 1 і 2 цієї Статті, а також для доповнення орієнтирів і показників у світлі розвитку технологій, таких як алгоритмічні вдосконалення або підвищення ефективності апаратного забезпечення, якщо це необхідно, щоб ці порогові значення відображали сучасний рівень розвитку.

Стаття 52

Процедура

1. Якщо загальноцільова модель ШІ відповідає умові, зазначеній у Статті 51(1), пункті (a), відповідний постачальник повідомляє Комісію без зволікань і в будь-якому випадку протягом двох тижнів після виконання цієї вимоги або після того, як стане відомо, що вона буде виконана. Таке повідомлення повинно містити інформацію, необхідну для підтвердження виконання відповідної вимоги. Якщо Комісії стає відомо про загальноцільову модель ШІ, що становить системні ризики, про яку її не було повідомлено, вона може вирішити позначити її як модель із системним ризиком.

2. Постачальник загальноцільової моделі ШІ, яка відповідає умові, зазначеній у Статті 51(1), пункті (a), може разом із своїм повідомленням надати достатньо обґрунтовані аргументи для підтвердження того, що, у виняткових випадках, незважаючи на відповідність цій вимозі, загальноцільова модель ШІ не становить системних ризиків через її специфічні характеристики і тому не повинна класифікуватися як загальноцільова модель ШІ із системним ризиком.

3. Якщо Комісія дійде висновку, що аргументи, подані відповідно до параграфа 2, не є достатньо обґрунтованими, і відповідний постачальник не зміг продемонструвати, що загальноцільова модель ШІ не становить системних ризиків через її специфічні характеристики, вона відхиляє ці аргументи, і загальноцільова модель ШІ вважається загальноцільовою моделлю ШІ із системним ризиком.

4. Комісія може позначити загальноцільову модель ШІ як таку, що становить системні ризики, ex officio або за обґрунтованим сповіщенням наукового комітету відповідно до Статті 90(1), пункту (a), на підставі критеріїв, викладених у Додатку XIII.

Комісія уповноважена приймати делеговані акти відповідно до Статті 97 з метою внесення змін до Додатка XIII шляхом уточнення та оновлення критеріїв, викладених у цьому Додатку.

5. За обґрунтованим запитом постачальника, модель якого була позначена як загальноцільова модель ШІ із системним ризиком відповідно до параграфа 4, Комісія бере до уваги такий запит і може вирішити переоцінити, чи може загальноцільова модель ШІ досі вважатися такою, що становить системні ризики, на підставі критеріїв, викладених у Додатку XIII. Такий запит повинен містити об'єктивні, детальні та нові підстави, що виникли після рішення про позначення. Постачальники можуть звертатися із запитом про переоцінку не раніше ніж через шість місяців після рішення про позначення. Якщо Комісія після своєї переоцінки вирішує зберегти позначення як загальноцільова модель ШІ із системним ризиком, постачальники можуть звертатися із запитом про переоцінку не раніше ніж через шість місяців після такого рішення.

6. Комісія забезпечує публікацію переліку загальноцільових моделей ШІ із системним ризиком і підтримує цей перелік в актуальному стані, без шкоди для необхідності дотримання та захисту прав інтелектуальної власності та конфіденційної ділової інформації або комерційної таємниці відповідно до права Союзу та національного законодавства.

РОЗДІЛ 2

Зобов'язання для постачальників моделей штучного інтелекту загального призначення

Стаття 53

Зобов'язання для постачальників загальноцільових моделей ШІ

1. Постачальники загальноцільових моделей ШІ зобов'язані:

(a) складати та підтримувати в актуальному стані технічну документацію моделі, включаючи процес її навчання та тестування та результати її оцінювання, яка повинна містити щонайменше інформацію, викладену в Додатку XI, з метою надання її на запит Офісу ШІ та національним компетентним органам;

(b) складати, підтримувати в актуальному стані та надавати інформацію та документацію постачальникам систем ШІ, які мають намір інтегрувати загальноцільову модель ШІ у свої системи ШІ. Без шкоди для необхідності дотримання та захисту прав інтелектуальної власності та конфіденційної ділової інформації або комерційної таємниці відповідно до права Союзу та національного законодавства, інформація та документація повинні:

(i) надавати постачальникам систем ШІ можливість добре розуміти можливості та обмеження загальноцільової моделі ШІ і дотримуватися своїх зобов'язань відповідно до цього Регламенту; та

(ii) містити щонайменше елементи, викладені в Додатку XII;

(c) запровадити політику дотримання права Союзу щодо авторського права та суміжних прав, зокрема для виявлення та дотримання, у тому

	числі шляхом застосування сучасних технологій, застереження прав, висловленого відповідно до Статті 4(3) Директиви (ЄС) 2019/790;
(d)	складати та оприлюднювати достатньо детальне резюме щодо вмісту, використаного для навчання загальноцільової моделі ШІ, відповідно до шаблону, наданого Офісом ШІ.

2. Зобов'язання, викладені в параграфі 1, пунктах (a) і (b), не застосовуються до постачальників моделей ШІ, що розповсюджуються за безкоштовною ліцензією з відкритим вихідним кодом, яка дозволяє доступ, використання, модифікацію та розповсюдження моделі, а параметри якої, включаючи ваги, інформацію про архітектуру моделі та інформацію про використання моделі, є загальнодоступними. Цей виняток не застосовується до загальноцільових моделей ШІ із системними ризиками.

3. Постачальники загальноцільових моделей ШІ співпрацюють у разі необхідності з Комісією та національними компетентними органами у здійсненні ними своїх компетенцій і повноважень відповідно до цього Регламенту.

4. Постачальники загальноцільових моделей ШІ можуть покладатися на кодекси практики у значенні Статті 56 для підтвердження відповідності зобов'язанням, викладеним у параграфі 1 цієї Статті, до опублікування гармонізованого стандарту. Дотримання європейських гармонізованих стандартів надає постачальникам презумпцію відповідності тією мірою, якою ці стандарти охоплюють зазначені зобов'язання. Постачальники загальноцільових моделей ШІ, які не дотримуються затвердженого кодексу практики або не дотримуються європейського гармонізованого стандарту, повинні продемонструвати альтернативні відповідні засоби дотримання для оцінки Комісією.

5. З метою сприяння дотриманню Додатка XI, зокрема пунктів 2(d) і (e) цього Додатка, Комісія уповноважена приймати делеговані акти відповідно до Статті 97 для деталізації методологій вимірювання та розрахунку з метою забезпечення порівнянної та перевіреної документації.

6. Комісія уповноважена приймати делеговані акти відповідно до Статті 97(2) для внесення змін до Додатків XI і XII у світлі розвитку технологій.

7. Будь-яка інформація або документація, отримана відповідно до цієї Статті, включаючи комерційну таємницю, підлягає обробці відповідно до зобов'язань щодо конфіденційності, викладених у Статті 78.

Стаття 54

Уповноважені представники постачальників загальноцільових моделей ШІ

1. До розміщення загальноцільової моделі ШІ на ринку Союзу постачальники, засновані в третіх країнах, за письмовим дорученням призначають уповноваженого представника, заснованого в Союзі.

2. Постачальник надає своєму уповноваженому представнику можливість виконувати завдання, визначені в дорученні, отриманому від постачальника.

3. Уповноважений представник виконує завдання, визначені в дорученні, отриманому від постачальника. На запит він надає копію доручення Офісу ШІ однією з офіційних мов інститутів Союзу. Для цілей цього Регламенту доручення надає уповноваженому представнику повноваження для виконання таких завдань:

(a) перевіряти, що технічна документація, зазначена в Додатку XI, була складена та що всі зобов'язання, зазначені в Статті 53 і, де застосовно, Статті 55, були виконані постачальником;

(b) зберігати копію технічної документації, зазначеної в Додатку XI, у розпорядженні Офісу ШІ та національних компетентних органів протягом 10 років після розміщення загальноцільової моделі ШІ на ринку, а також контактні дані постачальника, який призначив уповноваженого представника;

(c) надавати Офісу ШІ за обґрунтованим запитом всю інформацію та документацію, включаючи зазначену в пункті (b), необхідну для підтвердження відповідності зобов'язанням цієї Глави;

(d) співпрацювати з Офісом ШІ та компетентними органами за обґрунтованим запитом у будь-яких діях, що вживаються ними щодо загальноцільової моделі ШІ, у тому числі коли модель інтегрована у системи ШІ, розміщені на ринку або введені в експлуатацію в Союзі.

4. Доручення надає уповноваженому представнику повноваження бути адресатом звернень з боку Офісу ШІ або компетентних органів, на додаток до постачальника або замість нього, з усіх питань, пов'язаних із забезпеченням відповідності цьому Регламенту.

5. Уповноважений представник припиняє дію доручення, якщо він вважає або має підстави вважати, що постачальник діє всупереч своїм зобов'язанням відповідно до цього Регламенту. У такому випадку він також негайно інформує Офіс ШІ про припинення дії доручення та причини цього.

6. Зобов'язання, викладене в цій Статті, не застосовується до постачальників загальноцільових моделей ШІ, що розповсюджуються за безкоштовною ліцензією з відкритим вихідним кодом, яка дозволяє доступ, використання, модифікацію та розповсюдження моделі, а параметри якої, включаючи ваги, інформацію про архітектуру моделі та інформацію про використання моделі, є загальнодоступними, якщо тільки загальноцільові моделі ШІ не становлять системних ризиків.

РОЗДІЛ 3

Зобов'язання постачальників моделей штучного інтелекту загального призначення із системним ризиком

Стаття 55

Зобов'язання постачальників загальноцільових моделей ШІ із системним ризиком

1. На додаток до зобов'язань, перелічених у Статтях 53 і 54, постачальники загальноцільових моделей ШІ із системним ризиком зобов'язані:

(a) проводити оцінювання моделі відповідно до стандартизованих протоколів і інструментів, що відображають сучасний рівень розвитку, включаючи проведення та документування змагального тестування моделі з метою виявлення та зниження системних ризиків;

(b) оцінювати та пом'якшувати можливі системні ризики на рівні Союзу, включаючи їх джерела, що можуть виникати внаслідок розробки, розміщення на ринку або використання загальноцільових моделей ШІ із системним ризиком;

(c) відстежувати, документувати та повідомляти без невиправданої затримки Офісу ШІ та, у відповідних випадках, національним компетентним органам відповідну інформацію про серйозні інциденти та можливі коригувальні заходи щодо їх усунення;

(d) забезпечувати належний рівень захисту кібербезпеки загальноцільової моделі ШІ із системним ризиком та фізичної інфраструктури моделі.

2. Постачальники загальноцільових моделей ШІ із системним ризиком можуть покладатися на кодекси практики у значенні Статті 56 для підтвердження відповідності зобов'язанням, викладеним у параграфі 1 цієї Статті, до опублікування гармонізованого стандарту. Дотримання європейських гармонізованих стандартів надає постачальникам презумпцію відповідності тією мірою, якою ці стандарти охоплюють зазначені зобов'язання. Постачальники загальноцільових моделей ШІ із системними ризиками, які не дотримуються затвердженого кодексу практики або не дотримуються європейського гармонізованого стандарту, повинні продемонструвати альтернативні відповідні засоби дотримання для оцінки Комісією.

3. Будь-яка інформація або документація, отримана відповідно до цієї Статті, включаючи комерційну таємницю, підлягає обробці відповідно до зобов'язань щодо конфіденційності, викладених у Статті 78.

РОЗДІЛ 4

Кодекси поведінки

Стаття 56

Кодекси поведінки

1. Офіс зі штучного інтелекту заохочує та сприяє розробці кодексів поведінки на рівні Союзу з метою сприяння належному застосуванню цього Регламенту з урахуванням міжнародних підходів.

2. Офіс зі штучного інтелекту та Рада прагнуть забезпечити, щоб кодекси поведінки охоплювали щонайменше зобов'язання, передбачені статтями 53 і 55, включаючи такі питання:

(а) засоби забезпечення актуальності інформації, зазначеної в статті 53(1), пунктах (а) та (б), з урахуванням ринкових і технологічних змін;

(б) належний рівень деталізації зведеної інформації про контент, використаний для навчання;

(в) визначення виду та характеру системних ризиків на рівні Союзу, включаючи їхні джерела, де це доцільно;

(г) заходи, процедури та способи оцінки та управління системними ризиками на рівні Союзу, включаючи їх документування, що мають бути пропорційними ризикам, враховувати їхню серйозність і ймовірність та брати до уваги особливі виклики щодо подолання таких ризиків з огляду на можливі способи їх виникнення та матеріалізації вздовж ланцюга створення цінності у сфері ШІ.

3. Офіс зі штучного інтелекту може запрошувати всіх постачальників моделей штучного інтелекту загального призначення, а також відповідні національні компетентні органи до участі в розробці кодексів поведінки. Організації громадянського суспільства, промисловість, академічні кола та інші відповідні зацікавлені сторони, такі як постачальники нижчої ланки та незалежні експерти, можуть підтримувати цей процес.

4. Офіс зі штучного інтелекту та Рада прагнуть забезпечити, щоб кодекси поведінки чітко визначали свої конкретні цілі та містили зобов'язання або заходи, включаючи ключові показники ефективності за потреби, для забезпечення досягнення цих цілей, а також щоб вони належним чином враховували потреби та інтереси всіх заінтересованих сторін, включаючи осіб, яких це стосується, на рівні Союзу.

5. Офіс зі штучного інтелекту прагне забезпечити, щоб учасники кодексів поведінки регулярно звітували перед Офісом зі штучного інтелекту про виконання зобов'язань та вжиті заходи й їхні результати, у тому числі виміряні відносно ключових показників ефективності за потреби. Ключові показники ефективності та зобов'язання щодо звітності повинні відображати відмінності у розмірі та потужності між різними учасниками.

6. Офіс зі штучного інтелекту та Рада регулярно здійснюють моніторинг і оцінку досягнення учасниками цілей кодексів поведінки та їхнього внеску в належне застосування цього Регламенту. Офіс зі штучного інтелекту та Рада оцінюють, чи охоплюють кодекси поведінки зобов'язання, передбачені статтями 53 і 55, і регулярно здійснюють моніторинг і оцінку досягнення їхніх цілей. Вони публікують свою оцінку адекватності кодексів поведінки.

Комісія може шляхом імплементаційного акта затвердити кодекс поведінки та надати йому загальну чинність у межах Союзу. Такий імплементаційний акт приймається відповідно до процедури розгляду, зазначеної в статті 98(2).

7. Офіс зі штучного інтелекту може запрошувати всіх постачальників моделей штучного інтелекту загального призначення дотримуватися кодексів поведінки. Для постачальників моделей штучного інтелекту загального призначення, що не становлять системних ризиків, таке дотримання може бути обмежене зобов'язаннями, передбаченими статтею 53, якщо тільки вони прямо не заявляють про свій інтерес до приєднання до повного кодексу.

8. Офіс зі штучного інтелекту також за потреби заохочує та сприяє перегляду та адаптації кодексів поведінки, зокрема з огляду на стандарти, що з'являються. Офіс зі штучного інтелекту надає допомогу в оцінці наявних стандартів.

9. Кодекси поведінки повинні бути готові не пізніше 2 травня 2025 року. Офіс зі штучного інтелекту вживає необхідних заходів, включаючи запрошення постачальників відповідно до пункту 7.

Якщо до 2 серпня 2025 року кодекс поведінки не може бути остаточно доопрацьований, або якщо Офіс зі штучного інтелекту вважає його неналежним за результатами оцінки відповідно до пункту 6 цієї статті, Комісія може шляхом імплементаційних актів встановити спільні правила для виконання зобов'язань, передбачених статтями 53 і 55, включаючи питання, викладені в пункті 2 цієї статті. Такі імплементаційні акти приймаються відповідно до процедури розгляду, зазначеної в статті 98(2).

ГЛАВА VI

ЗАХОДИ НА ПІДТРИМКУ ІННОВАЦІЙ

Стаття 57

Регуляторні пісочниці зі штучного інтелекту

1. Держави-члени забезпечують, щоб їхні компетентні органи створили щонайменше одну регуляторну пісочницю зі штучного інтелекту на національному рівні, яка повинна бути запущена до 2 серпня 2026 року. Така пісочниця може також бути створена спільно з компетентними органами інших держав-членів. Комісія може надавати технічну підтримку, консультації та інструменти для створення та функціонування регуляторних пісочниць зі штучного інтелекту.

Зобов'язання відповідно до першого підпункту може також виконуватися шляхом участі в існуючій пісочниці за умови, що така участь забезпечує еквівалентний рівень національного охоплення для держав-членів, що беруть участь.

2. Можуть також створюватися додаткові регуляторні пісочниці зі штучного інтелекту на регіональному або місцевому рівні або спільно з компетентними органами інших держав-членів.

3. Європейський інспектор із захисту даних також може створити регуляторну пісочницю зі штучного інтелекту для інститутів, органів, служб і агентств Союзу та може виконувати ролі та завдання національних компетентних органів відповідно до цієї глави.

4. Держави-члени забезпечують, щоб компетентні органи, зазначені в пунктах 1 і 2, виділяли достатні ресурси для ефективного та своєчасного виконання цієї статті. У відповідних випадках національні компетентні органи співпрацюють з іншими відповідними органами та можуть допускати залучення інших учасників екосистеми штучного інтелекту. Ця стаття не впливає на інші регуляторні пісочниці, створені відповідно до права Союзу або національного права. Держави-члени забезпечують належний рівень співпраці між органами, що здійснюють нагляд за такими іншими пісочницями, та національними компетентними органами.

5. Регуляторні пісочниці зі штучного інтелекту, створені відповідно до пункту 1, забезпечують контрольоване середовище, що сприяє інноваціям та полегшує розробку, навчання, тестування та валідацію інноваційних систем штучного інтелекту протягом обмеженого часу до їх введення в обіг або введення в експлуатацію відповідно до конкретного плану пісочниці, погодженого між постачальниками або потенційними постачальниками та компетентним органом. Такі пісочниці можуть включати тестування в реальних умовах під наглядом у них.

6. Компетентні органи надають за потреби настанови, нагляд та підтримку в межах регуляторної пісочниці зі штучного інтелекту з метою виявлення ризиків, зокрема для основоположних прав, здоров'я та безпеки, тестування, заходів пом'якшення та їх ефективності стосовно зобов'язань і вимог цього Регламенту, а там, де це доречно, іншого права Союзу та національного права, що знаходиться під наглядом у пісочниці.

7. Компетентні органи надають постачальникам та потенційним постачальникам, що беруть участь у регуляторній пісочниці зі штучного інтелекту, настанови щодо регуляторних очікувань і того, як виконувати вимоги та зобов'язання, встановлені цим Регламентом.

На запит постачальника або потенційного постачальника системи штучного інтелекту компетентний орган надає письмовий доказ діяльності, успішно здійсненої в пісочниці. Компетентний орган також надає звіт про вихід із детальним описом діяльності, здійсненої в пісочниці, та пов'язаних результатів і навчальних висновків. Постачальники можуть використовувати таку документацію для

підтвердження своєї відповідності цьому Регламенту в процесі оцінки відповідності або в рамках відповідної діяльності з ринкового нагляду. У цьому відношенні звіти про вихід та письмовий доказ, надані національним компетентним органом, беруться до позитивного уваги органами ринкового нагляду та нотифікованими органами з метою прискорення процедур оцінки відповідності в розумній мірі.

8. З урахуванням положень про конфіденційність у статті 78 та за згодою постачальника або потенційного постачальника Комісія та Рада уповноважуються на доступ до звітів про вихід та беруть їх до уваги за потреби при виконанні своїх завдань відповідно до цього Регламенту. Якщо як постачальник або потенційний постачальник, так і національний компетентний орган прямо погоджуються, звіт про вихід може бути зроблений загальнодоступним через єдину інформаційну платформу, зазначену в цій статті.

9. Створення регуляторних пісочниць зі штучного інтелекту спрямоване на сприяння досягненню таких цілей:

(а) підвищення правової визначеності для досягнення відповідності регуляторним вимогам цього Регламенту або, де це доречно, іншого застосовного права Союзу та національного права;

(б) підтримка обміну найкращими практиками через співпрацю з органами, залученими до регуляторної пісочниці зі штучного інтелекту;

(в) заохочення інновацій і конкурентоспроможності та сприяння розвитку екосистеми штучного інтелекту;

(г) сприяння регуляторному навчанню на основі доказів;

(д) полегшення та прискорення доступу до ринку Союзу для систем штучного інтелекту, зокрема тих, що надаються МСП, включаючи стартапи.

10. Національні компетентні органи забезпечують, щоб тією мірою, якою інноваційні системи штучного інтелекту передбачають обробку персональних даних або іншим чином підпадають під наглядові повноваження інших національних органів або компетентних органів, що забезпечують або підтримують доступ до даних, національні органи захисту даних та ці інші національні або компетентні органи були пов'язані з функціонуванням регуляторної пісочниці зі штучного інтелекту та залучені до нагляду за такими аспектами в межах своїх відповідних завдань і повноважень.

11. Регуляторні пісочниці зі штучного інтелекту не впливають на наглядові або коригувальні повноваження компетентних органів, що здійснюють нагляд за пісочницями, у тому числі на регіональному або місцевому рівні. Будь-які значні ризики для здоров'я та безпеки та основоположних прав, виявлені в ході розробки та тестування таких систем штучного інтелекту, вимагають відповідного пом'якшення. Національні компетентні органи мають повноваження тимчасово або постійно призупиняти процес тестування або участь у пісочниці, якщо ефективне пом'якшення неможливе, та повідомляють Офіс зі штучного інтелекту про таке рішення. Національні

компетентні органи здійснюють свої наглядові повноваження в межах відповідного законодавства, використовуючи свої дискреційні повноваження при реалізації правових положень стосовно конкретного проекту регуляторної пісочниці зі штучного інтелекту з метою підтримки інновацій у сфері ШІ в Союзі.

12. Постачальники та потенційні постачальники, що беруть участь у регуляторній пісочниці зі штучного інтелекту, залишаються відповідальними відповідно до застосовного права Союзу та національного законодавства про відповідальність за будь-які збитки, завдані третім особам внаслідок експериментування в пісочниці. Однак за умови, що потенційні постачальники дотримуються конкретного плану та умов своєї участі та добросовісно виконують настанови національного компетентного органу, органи влади не накладають адміністративних штрафів за порушення цього Регламенту. Якщо інші компетентні органи, відповідальні за інше право Союзу та національне право, були активно залучені до нагляду за системою штучного інтелекту в пісочниці та надавали настанови щодо дотримання вимог, адміністративні штрафи щодо такого права не накладаються.

13. Регуляторні пісочниці зі штучного інтелекту розробляються та реалізуються таким чином, щоб там, де це доречно, вони сприяли транскордонній співпраці між національними компетентними органами.

14. Національні компетентні органи координують свою діяльність та співпрацюють у рамках Ради.

15. Національні компетентні органи інформують Офіс зі штучного інтелекту та Раду про створення пісочниці та можуть звертатися до них за підтримкою та настановами. Офіс зі штучного інтелекту робить загальнодоступним перелік запланованих та існуючих пісочниць і підтримує його в актуальному стані з метою заохочення більшої взаємодії в регуляторних пісочницях зі штучного інтелекту та транскордонної співпраці.

16. Національні компетентні органи подають щорічні звіти до Офісу зі штучного інтелекту та Ради, починаючи з одного року після створення регуляторної пісочниці зі штучного інтелекту та щороку після цього до її припинення, а також підсумковий звіт. Такі звіти містять інформацію про хід та результати реалізації цих пісочниць, включаючи найкращі практики, інциденти, засвоєні уроки та рекомендації щодо їх організації, а там, де це доречно, про застосування та можливий перегляд цього Регламенту, включаючи його делеговані та імплементаційні акти, і про застосування іншого права Союзу, що знаходиться під наглядом компетентних органів у пісочниці. Національні компетентні органи роблять ці щорічні звіти або їх резюме загальнодоступними онлайн. Комісія за потреби бере до уваги щорічні звіти при виконанні своїх завдань відповідно до цього Регламенту.

17. Комісія розробляє єдиний спеціальний інтерфейс, що містить всю відповідну інформацію, пов'язану з регуляторними пісочницями зі штучного інтелекту, щоб дати змогу зацікавленим сторонам взаємодіяти з регуляторними пісочницями зі штучного інтелекту та звертатися із запитами до компетентних органів, а також шукати необов'язкові настанови щодо відповідності інноваційних продуктів, послуг, бізнес-моделей, що впроваджують технології штучного інтелекту, відповідно до статті 62(1), пункту (в). Комісія активно координує дії з національними компетентними органами там, де це доречно.

Стаття 58

Детальні умови та функціонування регуляторних пісочниць зі штучного інтелекту

1. З метою уникнення фрагментації в межах Союзу Комісія приймає імплементаційні акти, що визначають детальні умови для створення, розробки, реалізації, функціонування та нагляду за регуляторними пісочницями зі штучного інтелекту. Імплементаційні акти включають спільні принципи з таких питань:

(а) критерії прийнятності та відбору для участі в регуляторній пісочниці зі штучного інтелекту;

(б) процедури подання заявки, участі, моніторингу, виходу та припинення регуляторної пісочниці зі штучного інтелекту, включаючи план пісочниці та звіт про вихід;

(в) умови, що застосовуються до учасників.

Такі імплементаційні акти приймаються відповідно до процедури розгляду, зазначеної в статті 98(2).

2. Імплементаційні акти, зазначені в пункті 1, забезпечують:

(а) щоб регуляторні пісочниці зі штучного інтелекту були відкриті для будь-якого постачальника, що подає заявку, або потенційного постачальника системи штучного інтелекту, який відповідає критеріям прийнятності та відбору, що мають бути прозорими та справедливими, і щоб національні компетентні органи повідомляли заявників про своє рішення протягом трьох місяців з дати подання заявки;

(б) щоб регуляторні пісочниці зі штучного інтелекту забезпечували широкий та рівний доступ і відповідали попиту на участь; постачальники та потенційні постачальники можуть також подавати заявки в партнерстві із суб'єктами розгортання та іншими відповідними третіми сторонами;

(в) щоб детальні умови та положення щодо регуляторних пісочниць зі штучного інтелекту максимально підтримували гнучкість для національних компетентних органів у створенні та функціонуванні їхніх регуляторних пісочниць зі штучного інтелекту;

(г) щоб доступ до регуляторних пісочниць зі штучного інтелекту був безкоштовним для МСП, включаючи стартапи, без шкоди для виняткових витрат, які національні компетентні органи можуть стягувати справедливим та пропорційним чином;

(д) щоб вони сприяли постачальникам та потенційним постачальникам за допомогою результатів навчання в регуляторних пісочницях зі штучного інтелекту у виконанні зобов'язань з оцінки відповідності відповідно до цього Регламенту та добровільному застосуванні кодексів поведінки, зазначених у статті 95;

(е) щоб регуляторні пісочниці зі штучного інтелекту сприяли залученню інших відповідних учасників екосистеми штучного інтелекту, таких як нотифіковані органи та організації зі стандартизації, МСП, включаючи стартапи, підприємства, новатори, об'єкти тестування та експериментування, науково-дослідні та експериментальні лабораторії та Європейські хаби цифрових інновацій, центри передового досвіду, окремі дослідники, з метою сприяння та полегшення співпраці з державним і приватним секторами;

(є) щоб процедури, процеси та адміністративні вимоги для подання заявки, відбору, участі та виходу з регуляторної пісочниці зі штучного інтелекту були простими, легко зрозумілими та чітко повідомлялися з метою полегшення участі МСП, включаючи стартапи, з обмеженими правовими та адміністративними можливостями, і були впорядковані в усьому Союзі для уникнення фрагментації, а також щоб участь у регуляторній пісочниці зі штучного інтелекту, створеній державою-членом або Європейським інспектором із захисту даних, взаємно та однаково визнавалася та мала однакові правові наслідки в усьому Союзі;

(ж) щоб участь у регуляторній пісочниці зі штучного інтелекту була обмежена строком, що відповідає складності та масштабу проекту, і який може бути продовжений національним компетентним органом;

(з) щоб регуляторні пісочниці зі штучного інтелекту сприяли розробці інструментів та інфраструктури для тестування, порівняльного аналізу, оцінки та пояснення вимірів систем штучного інтелекту, що є релевантними для регуляторного навчання,

таких як точність, надійність та кібербезпека, а також заходів для пом'якшення ризиків для основоположних прав та суспільства в цілому.

3. Потенційних постачальників у регуляторних пісочницях зі штучного інтелекту, зокрема МСП та стартапи, там де це доречно, скеровують до послуг, що передують розгортанню, таких як настанови щодо реалізації цього Регламенту, до інших послуг з доданою вартістю, таких як допомога зі стандартизаційними документами та сертифікацією, об'єктами тестування та експериментування, Європейськими хабами цифрових інновацій і центрами передового досвіду.

4. Якщо національні компетентні органи розглядають можливість дозволу тестування в реальних умовах під наглядом у рамках регуляторної пісочниці зі штучного інтелекту, яку планується створити відповідно до цієї статті, вони спеціально погоджують умови такого тестування і, зокрема, відповідні гарантії з учасниками з метою захисту основоположних прав, здоров'я та безпеки. У відповідних випадках вони співпрацюють з іншими національними компетентними органами з метою забезпечення узгодженої практики в усьому Союзі.

Стаття 59

Подальша обробка персональних даних для розробки певних систем штучного інтелекту в суспільних інтересах у регуляторній пісочниці зі штучного інтелекту

1. У регуляторній пісочниці зі штучного інтелекту персональні дані, законно зібрані для інших цілей, можуть оброблятися виключно з метою розробки, навчання та тестування певних систем штучного інтелекту в пісочниці за умови дотримання всіх таких умов:

(a) системи штучного інтелекту розробляються для захисту суттєвого суспільного інтересу органом публічної влади або іншою фізичною чи юридичною особою в одній або кількох з таких сфер:

(з) громадська безпека та охорона здоров'я населення, включаючи виявлення, профілактику, контроль та лікування захворювань і покращення систем охорони здоров'я;

(ii) високий рівень захисту та підвищення якості навколишнього середовища, захист біорізноманіття, захист від забруднення, заходи зеленого переходу, заходи щодо

пом'якшення наслідків зміни клімату та адаптації до неї;

(iii) енергетична сталість;

(iv) безпека та стійкість транспортних систем і мобільності, критичної інфраструктури та мереж;

(v) ефективність та якість державного управління та державних послуг;

(б) оброблювані дані є необхідними для дотримання однієї або кількох вимог, зазначених у главі III, розділ 2, де такі вимоги не можуть бути ефективно виконані шляхом обробки анонімізованих, синтетичних або інших неперсональних даних;

(в) існують ефективні механізми моніторингу для виявлення будь-яких високих ризиків для прав і свобод суб'єктів даних, як зазначено в статті 35 Регламенту (ЄС) 2016/679 та в статті 39 Регламенту (ЄС) 2018/1725, які можуть виникнути під час експериментування в пісочниці, а також механізми реагування для оперативного пом'якшення таких ризиків і, де необхідно, зупинки обробки;

(г) будь-які персональні дані, що підлягають обробці в контексті пісочниці, знаходяться в функціонально відокремленому, ізольованому та захищеному середовищі обробки даних під контролем потенційного постачальника, і лише уповноважені особи мають доступ до таких даних;

(д) постачальники можуть додатково передавати спочатку зібрані дані лише відповідно до законодавства Союзу про захист даних; будь-які персональні дані, створені в пісочниці, не можуть передаватися за межі пісочниці;

(е) будь-яка обробка персональних даних у контексті пісочниці не призводить до заходів або рішень, що стосуються суб'єктів даних, і не впливає на застосування їхніх прав, закріплених у праві Союзу про захист персональних даних;

(є) будь-які персональні дані, оброблені в контексті пісочниці, захищаються за допомогою відповідних технічних та організаційних заходів і видаляються після припинення участі в пісочниці або після закінчення строку зберігання персональних даних;

(ж) журнали обробки персональних даних у контексті пісочниці зберігаються протягом тривалості участі в пісочниці, якщо інше не передбачено правом Союзу або національним правом;

(з) повний та детальний опис процесу та обґрунтування навчання, тестування та валідації системи штучного інтелекту зберігається разом із результатами тестування як частина технічної документації, зазначеної в Додатку IV;

(и) коротке резюме проекту зі штучного інтелекту, розробленого в пісочниці, його цілей та очікуваних результатів публікується на веб-сайті компетентних органів; це зобов'язання не охоплює чутливі оперативні дані стосовно діяльності правоохоронних органів, органів прикордонного контролю, імміграційних або органів у справах надання притулку.

2. Для цілей запобігання, розслідування, виявлення або переслідування кримінальних правопорушень або виконання кримінальних покарань, включаючи захист від загроз публічній безпеці та їх запобігання, під контролем та відповідальністю правоохоронних органів обробка персональних даних у регуляторних пісочницях зі штучного інтелекту ґрунтується на конкретному праві Союзу або національному праві та підпорядковується тим самим кумулятивним умовам, що зазначені в пункті 1.

3. Пункт 1 не завдає шкоди праву Союзу або національному праву, що виключає обробку персональних даних для цілей, відмінних від тих, що прямо зазначені в такому праві, а також праву Союзу або національному праву, що встановлює підставу для обробки персональних даних, яка є необхідною для цілей розробки, тестування або навчання інноваційних систем штучного інтелекту або будь-якій іншій правовій підставі відповідно до права Союзу про захист персональних даних.

Стаття 60

Тестування високоризикових систем штучного інтелекту в реальних умовах за межами регуляторних пісочниць зі штучного інтелекту

1. Тестування високоризикових систем штучного інтелекту в реальних умовах за межами регуляторних пісочниць зі штучного інтелекту може проводитися постачальниками або потенційними постачальниками високоризикових систем штучного інтелекту, перелічених у Додатку III, відповідно до цієї статті та плану тестування в реальних умовах, зазначеного в цій статті, без шкоди для заборон відповідно до статті 5.

Комісія шляхом імплементаційних актів визначає детальні елементи плану тестування в реальних умовах. Такі імплементаційні акти приймаються відповідно до процедури розгляду, зазначеної в статті 98(2).

Цей пункт не завдає шкоди праву Союзу або національному праву щодо тестування в реальних умовах високоризикових систем штучного інтелекту, пов'язаних з продуктами, охопленими законодавством Союзу про гармонізацію, переліченим у Додатку I.

2. Постачальники або потенційні постачальники можуть проводити тестування високоризикових систем штучного інтелекту, зазначених у Додатку III, в реальних умовах у будь-який час до введення системи штучного інтелекту в обіг або введення в експлуатацію самостійно або у партнерстві з одним або кількома суб'єктами розгортання або потенційними суб'єктами розгортання.

3. Тестування високоризикових систем штучного інтелекту в реальних умовах відповідно до цієї статті не завдає шкоди будь-якому етичному огляду, що вимагається правом Союзу або національним правом.

4. Постачальники або потенційні постачальники можуть проводити тестування в реальних умовах лише за умови дотримання всіх таких умов:

(а)	постачальник або потенційний постачальник розробив план тестування в реальних умовах та подав його до органу ринкового нагляду в державі-члені, де планується проведення тестування в реальних умовах;
(б)	орган ринкового нагляду в державі-члені, де планується проведення тестування в реальних умовах, схвалив тестування в реальних умовах та план тестування в реальних умовах; якщо орган ринкового нагляду не надав відповідь протягом 30 днів, тестування в реальних умовах та план тестування в реальних умовах вважаються схваленими; якщо національне право не передбачає мовчазного схвалення, тестування в реальних умовах залишається предметом отримання дозволу;
(в)	постачальник або потенційний постачальник, за винятком постачальників або потенційних постачальників високоризикових систем штучного інтелекту, зазначених у пунктах 1, 6 та 7

Додатку III у сферах правоохоронної діяльності, міграції, надання притулку та управління прикордонним контролем, і високоризикових систем штучного інтелекту, зазначених у пункті 2 Додатку III, зареєстрував тестування в реальних умовах відповідно до статті 71(4) з унікальним ідентифікаційним номером, що діє в усьому Союзі, та з інформацією, зазначеною в Додатку IX; постачальник або потенційний постачальник високоризикових систем штучного інтелекту, зазначених у пунктах 1, 6 та 7 Додатку III у сферах правоохоронної діяльності, міграції, надання притулку та управління прикордонним контролем, зареєстрував тестування в реальних умовах у захищеному непублічному розділі бази даних ЄС відповідно до статті 49(4), пункту (г), з унікальним ідентифікаційним номером, що діє в усьому Союзі, та з інформацією, зазначеною в ньому; постачальник або потенційний постачальник високоризикових систем штучного інтелекту, зазначених у пункті 2 Додатку III, зареєстрував тестування в реальних умовах відповідно до статті 49(5);

(г) постачальник або потенційний постачальник, що проводить тестування в реальних умовах, є заснованим у Союзі або призначив юридичного представника, що є заснованим у Союзі;

(д) дані, зібрані та оброблені для цілей тестування в реальних умовах, можуть передаватися до третіх країн лише за умови впровадження відповідних та застосовних гарантій відповідно до права Союзу;

(е) тестування в реальних умовах не триває довше, ніж необхідно для досягнення його цілей, і в будь-якому випадку не довше шести місяців, які можуть бути продовжені на додатковий строк шести місяців за умови попереднього повідомлення постачальником або потенційним постачальником органу ринкового нагляду із поясненням необхідності такого продовження;

(є) суб'єкти тестування в реальних умовах, що є особами, які належать до вразливих груп внаслідок їхнього віку або інвалідності, відповідним чином захищені;

(ж) якщо постачальник або потенційний постачальник організовує тестування в реальних умовах у співпраці з одним або кількома суб'єктами розгортання або потенційними суб'єктами розгортання, останні поінформовані про всі аспекти тестування, що є релевантними для їхнього рішення щодо участі, та отримали відповідні інструкції з використання системи штучного інтелекту, зазначені в статті 13; постачальник або потенційний постачальник і суб'єкт розгортання або потенційний суб'єкт розгортання укладають угоду, що визначає їхні ролі та обов'язки з метою забезпечення дотримання положень щодо тестування в реальних умовах відповідно до цього Регламенту та відповідно до іншого застосовного права Союзу та національного права;

(з) суб'єкти тестування в реальних умовах надали поінформовану згоду відповідно до статті 61, або у випадку правоохоронної діяльності, де отримання поінформованої згоди перешкоджало б тестуванню системи штучного інтелекту, саме тестування та його результати в реальних умовах не мають будь-якого негативного впливу на суб'єктів, а їхні персональні дані видаляються після проведення тесту;

(и) тестування в реальних умовах ефективно контролюється постачальником або потенційним постачальником, а також суб'єктами розгортання або потенційними суб'єктами розгортання через осіб, що є відповідно кваліфікованими у відповідній сфері та мають необхідні можливості, підготовку та повноваження для виконання своїх завдань;

(і) прогнози, рекомендації або рішення системи штучного інтелекту можуть бути ефективно скасовані та проігноровані.

5. Будь-які суб'єкти тестування в реальних умовах або їхній законно призначений представник за потреби можуть без будь-якого заподіяння шкоди та без необхідності надавати будь-яке обґрунтування вийти з тестування в будь-який час шляхом відкликання своєї поінформованої згоди та можуть вимагати негайного та постійного видалення своїх персональних даних. Відкликання поінформованої згоди не впливає на вже здійснену діяльність.

6. Відповідно до статті 75 держави-члени наділяють свої органи ринкового нагляду повноваженнями вимагати від постачальників і потенційних постачальників надання інформації, проводити непередбачені дистанційні або виїзні перевірки та здійснювати контроль за проведенням тестування в реальних умовах і відповідних високоризикових систем штучного інтелекту. Органи ринкового нагляду використовують ці повноваження для забезпечення безпечного проведення тестування в реальних умовах.

7. Будь-який серйозний інцидент, виявлений в ході тестування в реальних умовах, повідомляється до національного органу ринкового нагляду відповідно до статті 73. Постачальник або потенційний постачальник вживає негайних заходів пом'якшення або, у разі неможливості, призупиняє тестування в реальних умовах до здійснення такого пом'якшення або іншим чином припиняє його. Постачальник або потенційний постачальник встановлює процедуру оперативного відкликання системи штучного інтелекту після такого припинення тестування в реальних умовах.

8. Постачальники або потенційні постачальники повідомляють національний орган ринкового нагляду в державі-члені, де планується проведення тестування в реальних умовах, про призупинення або припинення тестування в реальних умовах та про кінцеві результати.

9. Постачальник або потенційний постачальник несе відповідальність відповідно до застосовного права Союзу та національного законодавства про відповідальність за будь-які збитки, завдані в ході їхнього тестування в реальних умовах.

Стаття 61

Поінформована згода на участь у тестуванні в реальних умовах за межами регуляторних пісочниць зі штучного інтелекту

1. Для цілей тестування в реальних умовах відповідно до статті 60 від суб'єктів тестування отримується добровільно надана поінформована згода до їхньої участі в такому тестуванні та після того, як вони були належним чином поінформовані стислою, чіткою, релевантною та зрозумілою інформацією щодо:

(а) природи та цілей тестування в реальних умовах і можливих незручностей, що можуть бути пов'язані з їхньою участю;

(б) умов, за яких планується проведення тестування в реальних умовах, включаючи очікувану тривалість участі суб'єкта або суб'єктів;

(в) їхніх прав та гарантій щодо їхньої участі, зокрема їхнього права відмовитися від участі та права вийти з тестування в реальних умовах у будь-який час без будь-якого заподіяння шкоди та без необхідності надавати будь-яке обґрунтування;

(г) порядку подання запиту на скасування або ігнорування прогнозів, рекомендацій або рішень системи штучного інтелекту;

(д) унікального ідентифікаційного номера тестування в реальних умовах, що діє в усьому Союзі, відповідно до статті 60(4), пункту (в), та контактних даних постачальника або його юридичного представника, від якого можна отримати додаткову інформацію.

2. Поінформована згода датується та документується, а її копія надається суб'єктам тестування або їхньому юридичному представнику.

Стаття 62

Заходи для постачальників та суб'єктів розгортання, зокрема МСП, включаючи стартапи

1. Держави-члени вживають таких дій:

(а) надавати МСП, включаючи стартапи, що мають зареєстрований офіс або філію в Союзі, пріоритетний доступ до регуляторних пісочниць зі штучного інтелекту тією мірою, якою вони відповідають умовам прийнятності та критеріям відбору; пріоритетний доступ не перешкоджає доступу до регуляторної пісочниці зі штучного інтелекту інших МСП, включаючи стартапи, відмінних від тих, що зазначені в цьому пункті, за умови, що вони також відповідають умовам прийнятності та критеріям відбору;

(б) організовувати конкретні заходи з підвищення обізнаності та навчання щодо застосування цього Регламенту, пристосовані до потреб МСП, включаючи стартапи, суб'єктів розгортання та за потреби місцевих органів публічної влади;

(в) використовувати наявні спеціальні канали і де доцільно, створювати нові для комунікації з МСП, включаючи стартапи, суб'єктами розгортання, іншими новаторами та, де доцільно, місцевими органами публічної влади, для надання консультацій та відповідей на запити щодо реалізації цього Регламенту, у тому числі щодо участі в регуляторних пісочницях зі штучного інтелекту;

(г) сприяти участі МСП та інших відповідних зацікавлених сторін у процесі розробки стандартів.

2. Конкретні інтереси та потреби постачальників, що є МСП, включаючи стартапи, беруться до уваги при встановленні розміру зборів за оцінку відповідності відповідно до статті 43, зменшуючи ці збори пропорційно їхньому розміру, розміру ринку та іншим відповідним показникам.

3. Офіс зі штучного інтелекту вживає таких дій:

(а) надавати стандартизовані шаблони для сфер, охоплених цим Регламентом, як зазначено Радою в її запиті;

(б) розробляти та підтримувати єдину інформаційну платформу, що надає зручну для використання інформацію стосовно цього Регламенту для всіх операторів у Союзі;

(в) організовувати відповідні комунікаційні кампанії для підвищення обізнаності щодо зобов'язань, що виникають відповідно до цього Регламенту;

(г) оцінювати та сприяти конвергенції найкращих практик у процедурах державних закупівель стосовно систем штучного інтелекту.

Стаття 63

Відступи для конкретних операторів

1. Мікропідприємства в розумінні Рекомендації 2003/361/ЄС можуть виконувати певні елементи системи управління якістю, що вимагається статтею 17 цього Регламенту, у спрощений спосіб за умови, що вони не мають партнерських підприємств або пов'язаних підприємств у розумінні цієї Рекомендації. Для цього Комісія розробляє настанови щодо елементів системи управління якістю, які можуть виконуватися у спрощений спосіб з урахуванням потреб мікропідприємств, без впливу на рівень захисту або необхідність виконання вимог щодо високоризикових систем штучного інтелекту.

2. Пункт 1 цієї статті не тлумачиться як звільнення таких операторів від виконання будь-яких інших вимог або зобов'язань, встановлених цим Регламентом, включаючи ті, що встановлені статтями 9, 10, 11, 12, 13, 14, 15, 72 та 73.

ГЛАВА VII

УПРАВЛІННЯ

РОЗДІЛ 1

Управління на рівні Союзу

Стаття 64

Офіс зі штучного інтелекту

1. Комісія розвиває досвід та можливості Союзу у сфері штучного інтелекту через Офіс зі штучного інтелекту.

2. Держави-члени сприяють виконанню завдань, покладених на Офіс зі штучного інтелекту, як передбачено цим Регламентом.

Стаття 65

Заснування та структура Європейської ради з питань штучного інтелекту

1. Цим засновується Європейська рада з питань штучного інтелекту (далі — «Рада»).

2. Рада складається з одного представника від кожної держави-члена. Європейський інспектор із захисту даних бере участь у ролі спостерігача. Офіс зі штучного інтелекту також відвідує засідання Ради без участі в голосуванні. Інші національні органи та органи Союзу, установи або експерти можуть запрошуватися Радою на засідання в конкретних випадках, коли обговорювані питання є для них релевантними.

3. Кожен представник призначається своєю державою-членом на строк три роки з можливістю одноразового поновлення.

4. Держави-члени забезпечують, щоб їхні представники в Раді:

(а) мали відповідні компетенції та повноваження у своїй державі-члені, щоб активно сприяти досягненню завдань Ради, зазначених у статті 66;

(б) призначалися як єдина контактна точка стосовно Ради і, де доцільно, з урахуванням потреб держав-членів, як єдина контактна точка для зацікавлених сторін;

(в) були уповноважені сприяти послідовності та координації між національними компетентними органами у своїй державі-члені стосовно реалізації цього Регламенту, у тому числі шляхом збору відповідних даних та інформації для цілей виконання своїх завдань у Раді.

5. Призначені представники держав-членів приймають правила процедури Ради більшістю у дві третини. Правила процедури, зокрема, визначають процедури процесу відбору, тривалість мандату та деталізацію завдань Голови, детальні умови голосування та організацію діяльності Ради та її підгруп.

6. Рада засновує дві постійні підгрупи для забезпечення платформи для співпраці та обміну між органами ринкового нагляду та нотифікуючими органами з питань, пов'язаних відповідно з ринковим наглядом і нотифікованими органами.

Постійна підгрупа з ринкового нагляду має діяти як група адміністративного співробітництва (ADCO) для цього Регламенту в розумінні статті 30 Регламенту (ЄС) 2019/1020.

Рада може засновувати інші постійні або тимчасові підгрупи відповідно до обставин для цілей вивчення конкретних питань. Де це доречно, представники консультативного форуму, зазначеного в статті 67, можуть запрошуватися до таких підгруп або до конкретних засідань цих підгруп як спостерігачі.

7. Рада організовується та функціонує таким чином, щоб захистити об'єктивність та неупередженість її діяльності.

8. Рада очолюється одним із представників держав-членів. Офіс зі штучного інтелекту забезпечує секретаріат для Ради, скликає засідання на запит Голови та готує порядок денний відповідно до завдань Ради відповідно до цього Регламенту та правил її процедури.

Стаття 66

Завдання Ради

Рада надає консультації та допомогу Комісії та державам-членам з метою сприяння послідовному та ефективному застосуванню цього Регламенту. Для цього Рада може зокрема:

(а) сприяти координації між національними компетентними органами, відповідальними за застосування цього Регламенту, і у співпраці з відповідними органами ринкового нагляду та за їхньою згодою підтримувати спільну діяльність органів ринкового нагляду, зазначену в статті 74(11);

(б) збирати та обмінюватися технічним і регуляторним досвідом та найкращими практиками між державами-членами;

(в) надавати консультації щодо реалізації цього Регламенту, зокрема щодо застосування правил відносно моделей штучного інтелекту загального призначення;

(г) сприяти гармонізації адміністративних практик у державах-членах, у тому числі стосовно відступу від процедур оцінки відповідності, зазначених у статті 46, функціонування регуляторних пісочниць зі штучного інтелекту та тестування в реальних умовах, зазначеного в статтях 57, 59 та 60;

(д) на запит Комісії або за власною ініціативою, видавати рекомендації та письмові висновки з будь-яких відповідних питань, пов'язаних з

реалізацією цього Регламенту та його послідовним та ефективним застосуванням, включаючи:

(з) щодо розробки та застосування кодексів поведінки та кодексів практики відповідно до цього Регламенту, а також настанов Комісії;

(ii) оцінку та перегляд цього Регламенту відповідно до статті 112, у тому числі стосовно звітів про серйозні інциденти, зазначених у статті 73, і функціонування бази даних ЄС, зазначеної в статті 71, підготовку делегованих або імплементаційних актів, а також щодо можливих узгоджень цього Регламенту з законодавством Союзу про гармонізацію, переліченим у Додатку I;

(iii) щодо технічних специфікацій або існуючих стандартів стосовно вимог, встановлених у главі III, розділ 2;

(iv) щодо використання гармонізованих стандартів або спільних специфікацій, зазначених у статтях 40 та 41;

(v) тенденції, такі як глобальна конкурентоспроможність Європи у сфері

штучного інтелекту, впровадження штучного інтелекту в Союзі та розвиток цифрових навичок;

(vi) тенденції щодо типології ланцюгів створення цінності у сфері штучного інтелекту, що змінюється, зокрема щодо наслідків у плані підзвітності;

(vii) щодо потенційної необхідності внесення змін до Додатку III відповідно до статті 7, а також щодо потенційної необхідності можливого перегляду статті 5 відповідно до статті 112, з урахуванням відповідних наявних доказів та останніх технологічних розробок;

(е) підтримувати Комісію у сприянні грамотності у сфері штучного інтелекту, суспільній обізнаності та розумінні переваг, ризиків, гарантій та прав і обов'язків щодо використання систем штучного інтелекту;

(є) сприяти розробці спільних критеріїв та спільного розуміння серед учасників ринку та компетентних органів відповідних понять, передбачених цим Регламентом, у тому числі шляхом внеску в розробку орієнтирів;

(ж) співпрацювати за потреби з іншими інститутами, органами, службами та агентствами Союзу, а також відповідними експертними групами та мережами Союзу, зокрема у сферах безпеки продуктів, кібербезпеки, конкуренції, цифрових і

	медіапослуг, фінансових послуг, захисту прав споживачів, захисту даних та основоположних прав;
(з)	сприяти ефективній співпраці з компетентними органами третіх країн та з міжнародними організаціями;
(и)	надавати допомогу національним компетентним органам та Комісії у розвитку організаційного та технічного досвіду, необхідного для реалізації цього Регламенту, у тому числі шляхом внеску в оцінку потреб у підготовці для персоналу держав-членів, залученого до реалізації цього Регламенту;
(і)	надавати допомогу Офісу зі штучного інтелекту у підтримці національних компетентних органів у створенні та розвитку регуляторних пісочниць зі штучного інтелекту та сприяти співпраці та обміну інформацією між регуляторними пісочницями зі штучного інтелекту;
(ї)	робити внесок у розробку настановних документів та надавати відповідні консультації щодо неї;
(й)	консультувати Комісію з міжнародних питань щодо штучного інтелекту;
(к)	надавати Комісії висновки щодо кваліфікованих оповіщень стосовно моделей штучного інтелекту загального призначення;
(л)	отримувати висновки держав-членів щодо кваліфікованих оповіщень стосовно моделей штучного інтелекту загального призначення, а також щодо національного досвіду та практик моніторингу та застосування систем штучного інтелекту, зокрема систем, що інтегрують моделі штучного інтелекту загального призначення.

Стаття 67

Консультативний форум

1. Засновується консультативний форум для надання технічного досвіду та консультування Ради та Комісії, а також для сприяння виконанню їхніх завдань відповідно до цього Регламенту.

2. Склад членів консультативного форуму представляє збалансований відбір зацікавлених сторін, включаючи промисловість, стартапи, МСП, громадянське суспільство та академічні кола. Склад членів консультативного форуму є збалансованим щодо комерційних та некомерційних інтересів, а в категорії комерційних інтересів — щодо МСП та інших підприємств.

3. Комісія призначає членів консультативного форуму відповідно до критеріїв, викладених у пункті 2, з числа зацікавлених сторін із визнаним досвідом у сфері штучного інтелекту.

4. Строк повноважень членів консультативного форуму становить два роки, який може бути продовжений не більше ніж до чотирьох років.

5. Агентство з основоположних прав, ENISA, Європейський комітет зі стандартизації (CEN), Європейський комітет зі стандартизації в електротехніці (CENELEC) та Європейський інститут стандартів електрозв'язку (ETSI) є постійними членами консультативного форуму.

6. Консультативний форум розробляє свої правила процедури. Він обирає двох співголів зі своїх членів відповідно до критеріїв, викладених у пункті 2. Строк повноважень співголів становить два роки з можливістю одноразового поновлення.

7. Консультативний форум проводить засідання не менше двох разів на рік. Консультативний форум може запрошувати експертів та інших зацікавлених сторін на свої засідання.

8. Консультативний форум може готувати висновки, рекомендації та письмові матеріали на запит Ради або Комісії.

9. Консультативний форум може засновувати постійні або тимчасові підгрупи відповідно до обставин для цілей розгляду конкретних питань, пов'язаних із цілями цього Регламенту.

10. Консультативний форум готує щорічний звіт про свою діяльність. Цей звіт робиться загальнодоступним.

Стаття 68

Наукова рада незалежних експертів

1. Комісія шляхом імплементаційного акта встановлює положення щодо заснування наукової ради незалежних експертів (далі — «наукова рада»), призначеної для підтримки правозастосовної діяльності відповідно до цього Регламенту. Такий імплементаційний акт приймається відповідно до процедури розгляду, зазначеної в статті 98(2).

2. Наукова рада складається з експертів, відібраних Комісією на підставі сучасного наукового або технічного досвіду у сфері штучного інтелекту, необхідного для завдань, визначених у пункті 3, та здатних підтвердити відповідність усім таким умовам:

(а)	мати особливий досвід та компетентність і науковий або технічний досвід у сфері штучного інтелекту;
(б)	незалежність від будь-якого постачальника систем штучного інтелекту або моделей штучного інтелекту загального призначення;
(в)	здатність виконувати діяльність сумлінно, точно та об'єктивно.

Комісія у консультації з Радою визначає кількість експертів у раді відповідно до необхідних потреб і забезпечує справедливе гендерне та географічне представництво.

3. Наукова рада консультує та підтримує Офіс зі штучного інтелекту, зокрема стосовно таких завдань:

(a) підтримка реалізації та застосування цього Регламенту стосовно моделей і систем штучного інтелекту загального призначення, зокрема шляхом:

(i) оповіщення Офісу зі штучного інтелекту про можливі системні ризики на рівні Союзу від моделей штучного інтелекту загального призначення відповідно до статті 90;

(ii) внеску в розробку інструментів та методологій для оцінки можливостей моделей і систем штучного інтелекту загального призначення, у тому числі через орієнтири;

(iii) надання консультацій щодо класифікації моделей штучного інтелекту загального призначення із системним ризиком;

(iv) надання консультацій щодо класифікації різних моделей і систем штучного інтелекту загального призначення;

(v) внеску в розробку інструментів та шаблонів;

(б) підтримка роботи органів ринкового нагляду на їхній запит;

(в)	підтримка транскордонної діяльності з ринкового нагляду, зазначеної в статті 74(11), без шкоди для повноважень органів ринкового нагляду;
(г)	підтримка Офісу зі штучного інтелекту у виконанні його обов'язків у контексті захисної процедури Союзу відповідно до статті 81.

4. Експерти наукової ради виконують свої завдання неупереджено та об'єктивно і забезпечують конфіденційність інформації та даних, отриманих при виконанні своїх завдань та провадженні діяльності. Вони не шукають та не отримують жодних вказівок від будь-кого при виконанні своїх завдань відповідно до пункту 3. Кожен експерт складає декларацію про інтереси, яка робиться загальнодоступною. Офіс зі штучного інтелекту встановлює системи та процедури для активного управління та запобігання потенційним конфліктам інтересів.

5. Імплементаційний акт, зазначений у пункті 1, включає положення щодо умов, процедур та детальних умов для наукової ради та її членів щодо видачі оповіщень та звернення за допомогою до Офісу зі штучного інтелекту для виконання завдань наукової ради.

Стаття 69

Доступ держав-членів до пулу експертів

1. Держави-члени можуть залучати експертів наукової ради для підтримки своєї правозастосовної діяльності відповідно до цього Регламенту.

2. Від держав-членів може вимагатися сплата зборів за консультації та підтримку, що надаються експертами. Структура та рівень зборів, а також масштаб та структура відшкодовуваних витрат встановлюються в імплементаційному акті, зазначеному в статті 68(1), з урахуванням цілей належної реалізації цього Регламенту, економічної ефективності та необхідності забезпечення ефективного доступу до експертів для всіх держав-членів.

3. Комісія сприяє своєчасному доступу держав-членів до експертів за потреби та забезпечує, щоб поєднання підтримувальної діяльності, здійснюваної службою підтримки тестування штучного інтелекту Союзу відповідно до статті 84, та експертів відповідно до цієї статті було ефективно організоване та забезпечувало найкращу можливу додану вартість.

РОЗДІЛ 2

Національні компетентні органи

Стаття 70

Призначення національних компетентних органів та єдиних контактних точок

1. Кожна держава-член засновує або призначає як національні компетентні органи щонайменше один нотифікуючий орган та щонайменше один орган ринкового нагляду для цілей цього Регламенту. Ці національні компетентні органи здійснюють свої повноваження незалежно, неупереджено та без упередженості з метою захисту об'єктивності своєї діяльності та завдань і для забезпечення застосування та реалізації цього Регламенту. Члени цих органів утримуються від будь-яких дій, несумісних із їхніми обов'язками. За умови дотримання цих принципів, така діяльність та завдання можуть виконуватися одним або кількома призначеними органами відповідно до організаційних потреб держави-члена.

2. Держави-члени повідомляють Комісію про ідентичність нотифікуючих органів та органів ринкового нагляду і завдання цих органів, а також про будь-які наступні зміни до них. Держави-члени роблять загальнодоступною інформацію про те, як можна зв'язатися з компетентними органами та єдиними контактними точками, через засоби електронного зв'язку до 2 серпня 2025 року. Держави-члени призначають орган ринкового нагляду для виконання функцій єдиної контактної точки для цього Регламенту та повідомляють Комісію про ідентичність єдиної контактної точки. Комісія робить перелік єдиних контактних точок загальнодоступним.

3. Держави-члени забезпечують, щоб їхні національні компетентні органи мали достатні технічні, фінансові та людські ресурси, а також інфраструктуру для ефективного виконання своїх завдань відповідно до цього Регламенту. Зокрема, національні компетентні органи повинні мати достатню кількість постійно доступного персоналу, компетенції та досвід якого включатимуть поглиблене розуміння технологій штучного інтелекту, даних та обчислення даних, захисту персональних даних, кібербезпеки, основоположних прав, ризиків для здоров'я та безпеки та знання існуючих стандартів і правових вимог. Держави-члени щорічно оцінюють і за необхідності оновлюють вимоги до компетенцій та ресурсів, зазначених у цьому пункті.

4. Національні компетентні органи вживають відповідних заходів для забезпечення належного рівня кібербезпеки.

5. При виконанні своїх завдань національні компетентні органи діють відповідно до зобов'язань щодо конфіденційності, встановлених у статті 78.

6. До 2 серпня 2025 року і раз на два роки після цього держави-члени звітують Комісії про стан фінансових та людських ресурсів національних компетентних органів з оцінкою їхньої достатності. Комісія передає цю інформацію Раді для обговорення та можливих рекомендацій.

7. Комісія сприяє обміну досвідом між національними компетентними органами.

8. Національні компетентні органи можуть надавати настанови та консультації щодо реалізації цього Регламенту, зокрема МСП, включаючи стартапи, беручи до уваги настанови та консультації Ради та Комісії за потреби. Щоразу, коли національні компетентні органи мають намір надавати настанови та консультації щодо системи штучного інтелекту в сферах, охоплених іншим правом Союзу, з національними компетентними органами відповідно до такого права Союзу консультуються за потреби.

9. Якщо інститути, органи, служби або агентства Союзу підпадають під сферу застосування цього Регламенту, Європейський інспектор із захисту даних виконує функції компетентного органу для їхнього нагляду.

ГЛАВА VIII

БАЗА ДАНИХ ЄС ДЛЯ ВИСОКОРИЗИКОВИХ СИСТЕМ ШТУЧНОГО ІНТЕЛЕКТУ

Стаття 71

База даних ЄС для високоризикових систем штучного інтелекту, перелічених у Додатку III

1. Комісія у співпраці з державами-членами створює та підтримує базу даних ЄС, що містить інформацію, зазначену в пунктах 2 та 3 цієї статті, стосовно високоризикових систем штучного інтелекту, зазначених у статті 6(2), зареєстрованих відповідно до статей 49 та 60, та систем штучного інтелекту, що не вважаються високоризиковими відповідно до статті 6(3) та зареєстровані відповідно до статті 6(4) та статті 49. При встановленні функціональних специфікацій такої бази даних Комісія консультується з відповідними експертами, а при оновленні функціональних специфікацій такої бази даних — з Радою.

2. Дані, перелічені в розділах A та B Додатку VIII, вносяться до бази даних ЄС постачальником або, де це застосовно, уповноваженим представником.

3. Дані, перелічені в розділі C Додатку VIII, вносяться до бази даних ЄС суб'єктом розгортання, що є або діє від імені органу публічної влади, агентства або установи, відповідно до статті 49(3) та (4).

4. За винятком розділу, зазначеного в статті 49(4) та статті 60(4), пункті (в), інформація, що міститься в базі даних ЄС, зареєстрована відповідно до статті 49, є доступною та загальнодоступною у зручний для користувача спосіб. Інформація має бути легко для навігації та машиночитаною. Інформація, зареєстрована відповідно до статті 60, є доступною лише для органів ринкового нагляду та Комісії, якщо тільки потенційний постачальник або постачальник не дав згоди на також зробити інформацію доступною для громадськості.

5. База даних ЄС містить персональні дані лише тою мірою, якою це необхідно для збору та обробки інформації відповідно до цього Регламенту. Така інформація включає імена та контактні дані фізичних осіб, відповідальних за реєстрацію системи та уповноважених представляти постачальника або суб'єкта розгортання залежно від обставин.

6. Комісія є контролером бази даних ЄС. Вона надає постачальникам, потенційним постачальникам та суб'єктам розгортання достатню технічну та адміністративну підтримку. База даних ЄС відповідає застосовним вимогам доступності.

ГЛАВА IX

МОНІТОРИНГ ПІСЛЯ ВВЕДЕННЯ В ОБІГ, ОБМІН ІНФОРМАЦІЄЮ ТА РИНКОВИЙ НАГЛЯД

РОЗДІЛ 1

Моніторинг після введення в обіг

Стаття 72

Пост-ринковий моніторинг постачальниками та план пост-ринкового моніторингу для високоризикових систем штучного інтелекту

1. Постачальники засновують та документують систему пост-ринкового моніторингу у спосіб, що є пропорційним характеру технологій штучного інтелекту та ризикам високоризикової системи штучного інтелекту.

2. Система пост-ринкового моніторингу активно та систематично збирає, документує та аналізує відповідні дані, які можуть надаватися суб'єктами розгортання або збиратися з інших джерел, щодо продуктивності високоризикових систем штучного інтелекту протягом усього їхнього строку служби, і які дозволяють постачальнику оцінювати постійну відповідність систем штучного інтелекту вимогам, встановленим у главі III, розділ 2. Де це доречно, пост-ринковий моніторинг включає аналіз взаємодії з іншими системами штучного інтелекту. Це зобов'язання не охоплює чутливі оперативні дані суб'єктів розгортання, що є правоохоронними органами.

3. Система пост-ринкового моніторингу ґрунтується на плані пост-ринкового моніторингу. План пост-ринкового моніторингу є частиною технічної документації, зазначеної в Додатку IV. Комісія приймає імплементаційний акт, що встановлює детальні положення для розробки шаблону плану пост-ринкового моніторингу та переліку елементів, що мають бути включені до плану, до 2 лютого 2026 року. Такий імплементаційний акт приймається відповідно до процедури розгляду, зазначеної в статті 98(2).

4. Для високоризикових систем штучного інтелекту, охоплених законодавством Союзу про гармонізацію, переліченим у розділі A Додатку I, де система та план пост-ринкового моніторингу вже встановлені відповідно до такого законодавства, з метою забезпечення послідовності, уникнення дублювань та мінімізації додаткового навантаження, постачальники мають можливість інтегрувати за потреби необхідні елементи, описані в пунктах 1, 2 та 3, використовуючи шаблон, зазначений у пункті 3, у системи та плани, що вже існують відповідно до такого законодавства, за умови, що це забезпечує рівноцінний рівень захисту.

Перший підпункт цього пункту також застосовується до високоризикових систем штучного інтелекту, зазначених у пункті 5 Додатку III, введених в обіг або введених в експлуатацію фінансовими установами, що підпадають під вимоги законодавства Союзу про фінансові послуги щодо їхнього внутрішнього управління, заходів або процесів.

РОЗДІЛ 2

Обмін інформацією про серйозні інциденти

Стаття 73

Повідомлення про серйозні інциденти

1. Постачальники високоризикових систем штучного інтелекту, введених в обіг Союзу, повідомляють про будь-який серйозний інцидент до органів ринкового нагляду держав-членів, де такий інцидент стався.

2. Звіт, зазначений у пункті 1, надається негайно після того, як постачальник встановив причинно-наслідковий зв'язок між системою штучного інтелекту та серйозним інцидентом або обґрунтовану ймовірність такого зв'язку, і в будь-якому випадку не пізніше ніж через 15 днів після того, як постачальник або, де це застосовно, суб'єкт розгортання, дізнається про серйозний інцидент.

Строк подання звіту, зазначеного в першому підпункті, враховує серйозність серйозного інциденту.

3. Незважаючи на пункт 2 цієї статті, у разі широкого порушення або серйозного інциденту, як визначено в статті 3, пункті (49)(б), звіт, зазначений у пункті 1 цієї статті, надається негайно, і не пізніше ніж через два дні після того, як постачальник або, де це застосовно, суб'єкт розгортання дізнається про такий інцидент.

4. Незважаючи на пункт 2, у разі смерті особи звіт надається негайно після того, як постачальник або суб'єкт розгортання встановив або одразу після виникнення підозри щодо причинно-наслідкового зв'язку між високоризиковою системою штучного інтелекту та серйозним інцидентом, але не пізніше ніж через 10 днів після дати, коли постачальник або, де це застосовно, суб'єкт розгортання дізнається про серйозний інцидент.

5. Де це необхідно для забезпечення своєчасного звітування, постачальник або, де це застосовно, суб'єкт розгортання, може подати початковий звіт, що є неповним, з подальшим поданням повного звіту.

6. Після повідомлення про серйозний інцидент відповідно до пункту 1 постачальник без зволікання проводить необхідні розслідування стосовно серйозного інциденту та відповідної системи штучного інтелекту. Це включає оцінку ризику інциденту та коригувальні заходи.

Постачальник співпрацює з компетентними органами, а там де це доречно, з відповідним нотифікованим органом, під час розслідувань, зазначених у першому підпункті, і не проводить жодного розслідування, що передбачає зміну відповідної системи штучного інтелекту у спосіб, що може вплинути на будь-яку наступну оцінку причин інциденту, до інформування компетентних органів про такі дії.

7. Після отримання повідомлення про серйозний інцидент, зазначений у статті 3, пункті (49)(в), відповідний орган ринкового нагляду інформує національні органи публічної влади або установи, зазначені в статті 77(1). Комісія розробляє спеціальні настанови для полегшення дотримання зобов'язань, встановлених у пункті 1 цієї статті. Такі настанови видаються до 2 серпня 2025 року та регулярно переоцінюються.

8. Орган ринкового нагляду вживає відповідних заходів, як передбачено в статті 19 Регламенту (ЄС) 2019/1020, протягом семи днів з дати отримання повідомлення, зазначеного в пункті 1 цієї статті, та дотримується процедур повідомлення, передбачених у цьому Регламенті.

9. Для високоризикових систем штучного інтелекту, зазначених у Додатку III, що введені в обіг або введені в експлуатацію постачальниками, що підпадають під законодавчі акти Союзу, що встановлюють зобов'язання щодо звітності, еквівалентні тим, що встановлені в цьому Регламенті, повідомлення про серйозні інциденти обмежується тими, що зазначені в статті 3, пункті (49)(в).

10. Для високоризикових систем штучного інтелекту, що є компонентами безпеки пристроїв або самі є пристроями, охопленими Регламентами (ЄС) 2017/745 та (ЄС) 2017/746, повідомлення про серйозні інциденти обмежується тими, що зазначені в статті 3, пункті (49)(в) цього Регламенту, та надсилається до національного компетентного органу, обраного для цієї мети державами-членами, де стався інцидент.

11. Національні компетентні органи негайно повідомляють Комісію про будь-який серйозний інцидент, незалежно від того, чи вжили вони заходів щодо нього, відповідно до статті 20 Регламенту (ЄС) 2019/1020.

РОЗДІЛ 3

Застосування

Стаття 74

Ринковий нагляд та контроль систем штучного інтелекту на ринку Союзу

1. Регламент (ЄС) 2019/1020 застосовується до систем штучного інтелекту, охоплених цим Регламентом. Для цілей ефективного застосування цього Регламенту:

(а)	будь-яке посилання на суб'єкта господарювання відповідно до Регламенту (ЄС) 2019/1020 розуміється як таке, що включає всіх операторів, визначених у статті 2(1) цього Регламенту;
(б)	будь-яке посилання на продукт відповідно до Регламенту (ЄС) 2019/1020 розуміється як таке, що включає всі системи штучного інтелекту, що підпадають під сферу застосування цього Регламенту.

2. В рамках своїх зобов'язань щодо звітності відповідно до статті 34(4) Регламенту (ЄС) 2019/1020 органи ринкового нагляду щорічно звітують Комісії та відповідним національним органам конкуренції про будь-яку інформацію, виявлену в ході діяльності з ринкового нагляду, яка може становити потенційний інтерес для застосування права Союзу щодо правил конкуренції. Вони також щорічно звітують Комісії про використання заборонених практик, що мали місце протягом того року, та про вжиті заходи.

3. Для високоризикових систем штучного інтелекту, пов'язаних з продуктами, охопленими законодавством Союзу про гармонізацію, переліченим у розділі А Додатку I, органом ринкового нагляду для цілей цього Регламенту є орган, відповідальний за діяльність з ринкового нагляду, призначений відповідно до таких правових актів.

Як відступ від першого підпункту, і за відповідних обставин, держави-члени можуть призначити інший відповідний орган для виконання функцій органу ринкового нагляду за умови забезпечення координації з відповідними галузевими органами ринкового нагляду, відповідальними за застосування законодавства Союзу про гармонізацію, переліченого в Додатку I.

4. Процедури, зазначені в статтях 79–83 цього Регламенту, не застосовуються до систем штучного інтелекту, пов'язаних з продуктами, охопленими законодавством Союзу про гармонізацію, переліченим у розділі А Додатку I, де такі правові акти вже передбачають процедури, що забезпечують рівноцінний рівень захисту та мають ту саму мету. У таких випадках замість них застосовуються відповідні галузеві процедури.

5. Без шкоди для повноважень органів ринкового нагляду відповідно до статті 14 Регламенту (ЄС) 2019/1020, з метою забезпечення ефективного застосування цього Регламенту органи ринкового нагляду можуть здійснювати повноваження, зазначені в статті 14(4), пунктах (г) та (й), цього Регламенту, дистанційно за потреби.

6. Для високоризикових систем штучного інтелекту, введених в обіг, введених в експлуатацію або використовуваних фінансовими установами, що регулюються законодавством Союзу про фінансові послуги, органом ринкового нагляду для цілей цього Регламенту є відповідний національний орган,

відповідальний за фінансовий нагляд за цими установами відповідно до такого законодавства, тією мірою, якою введення в обіг, введення в експлуатацію або використання системи штучного інтелекту безпосередньо пов'язане з наданням цих фінансових послуг.

7. Як відступ від пункту 6, за відповідних обставин і за умови забезпечення координації, держава-член може визначити інший відповідний орган як орган ринкового нагляду для цілей цього Регламенту.

Національні органи ринкового нагляду, що здійснюють нагляд за регульованими кредитними установами, що регулюються відповідно до Директиви 2013/36/ЄС, які беруть участь у Єдиному наглядовому механізмі, заснованому Регламентом (ЄС) № 1024/2013, повинні без зволікання повідомляти Європейський центральний банк про будь-яку інформацію, виявлену в ході їхньої діяльності з ринкового нагляду, яка може становити потенційний інтерес для пруденційних наглядових завдань Європейського центрального банку, визначених у цьому Регламенті.

8. Для високоризикових систем штучного інтелекту, перелічених у пункті 1 Додатку III до цього Регламенту, тією мірою, якою системи використовуються для правоохоронних цілей, управління кордонами та правосуддя і демократії, і для високоризикових систем штучного інтелекту, перелічених у пунктах 6, 7 та 8 Додатку III до цього Регламенту, держави-члени призначають як органи ринкового нагляду для цілей цього Регламенту або компетентні наглядові органи із захисту даних відповідно до Регламенту (ЄС) 2016/679 або Директиви (ЄС) 2016/680, або будь-який інший орган, призначений відповідно до тих самих умов, встановлених у статтях 41–44 Директиви (ЄС) 2016/680. Діяльність з ринкового нагляду жодним чином не впливає на незалежність судових органів або іншим чином не втручається в їхню діяльність під час виконання ними судових функцій.

9. Якщо інститути, органи, служби або агентства Союзу підпадають під сферу застосування цього Регламенту, Європейський інспектор із захисту даних виконує функції органу ринкового нагляду для них, за винятком відносин із Судом Справедливості Європейського Союзу під час виконання ним судових функцій.

10. Держави-члени сприяють координації між органами ринкового нагляду, призначеними відповідно до цього Регламенту, та іншими відповідними національними органами або установами, що здійснюють нагляд за застосуванням законодавства Союзу про гармонізацію, переліченого в Додатку I, або іншого права Союзу, яке може бути релевантним для високоризикових систем штучного інтелекту, зазначених у Додатку III.

11. Органи ринкового нагляду та Комісія можуть пропонувати спільну діяльність, включаючи спільні розслідування, що проводяться або органами ринкового нагляду, або органами ринкового нагляду спільно з Комісією, що мають на меті сприяння дотриманню вимог, виявлення невідповідності, підвищення обізнаності або надання настанов стосовно цього Регламенту щодо конкретних категорій високоризикових систем штучного інтелекту, що виявляються такими, що становлять серйозний ризик у двох або більше державах-членах відповідно до статті 9 Регламенту (ЄС) 2019/1020. Офіс зі штучного інтелекту надає координаційну підтримку для спільних розслідувань.

12. Без шкоди для повноважень, передбачених у Регламенті (ЄС) 2019/1020, і де це доречно та обмежено тим, що необхідно для виконання їхніх завдань, постачальники надають органам ринкового нагляду повний доступ до документації, а також до навчальних, валідаційних та тестувальних наборів даних, використаних для розробки високоризикових систем штучного інтелекту, у тому числі за потреби та з урахуванням заходів безпеки через прикладні програмні інтерфейси (API) або інші відповідні технічні засоби та інструменти, що дозволяють дистанційний доступ.

13. Органам ринкового нагляду надається доступ до вихідного коду системи штучного інтелекту за мотивованим запитом і лише тоді, коли виконані обидві такі умови:

(а) доступ до вихідного коду є необхідним для оцінки відповідності високоризикової системи штучного інтелекту вимогам, встановленим у главі III, розділ 2; та

(б) процедури тестування або аудиту та перевірки на основі даних та документації, наданих постачальником, були вичерпані або виявилися недостатніми.

14. Будь-яка інформація або документація, отримана органами ринкового нагляду, обробляється відповідно до зобов'язань щодо конфіденційності, встановлених у статті 78.

Стаття 75

Взаємна допомога, ринковий нагляд та контроль систем штучного інтелекту загального призначення

1. Якщо система штучного інтелекту базується на моделі штучного інтелекту загального призначення і модель та система розроблені одним постачальником, Офіс зі штучного інтелекту має повноваження з моніторингу та нагляду за дотриманням цією системою штучного інтелекту зобов'язань відповідно до цього Регламенту. Для виконання своїх завдань з моніторингу та нагляду Офіс зі штучного інтелекту має всі повноваження органу ринкового нагляду, передбачені в цьому розділі та Регламенті (ЄС) 2019/1020.

2. Якщо відповідні органи ринкового нагляду мають достатні підстави вважати, що системи штучного інтелекту загального призначення, що можуть безпосередньо використовуватися суб'єктами розгортання щонайменше для однієї мети, що класифікується як високоризикова відповідно до цього Регламенту, не відповідають вимогам, встановленим у цьому Регламенті, вони співпрацюють з Офісом зі штучного інтелекту для проведення оцінок відповідності та відповідно інформують Раду та інші органи ринкового нагляду.

3. Якщо орган ринкового нагляду не може завершити своє розслідування щодо високоризикової системи штучного інтелекту через неможливість доступу до певної інформації, пов'язаної з моделлю штучного інтелекту загального призначення, незважаючи на всі відповідні зусилля щодо отримання такої інформації, він може подати мотивований запит до Офісу зі штучного інтелекту, на підставі якого доступ до такої інформації забезпечується примусово. У такому випадку Офіс зі штучного інтелекту надає органу-заявнику без зволікання і в будь-якому випадку протягом 30 днів будь-яку інформацію, яку Офіс зі штучного інтелекту вважає релевантною для встановлення того, чи є висококризова система штучного інтелекту невідповідною. Органи ринкового нагляду забезпечують конфіденційність інформації, яку вони отримують відповідно до статті 78 цього Регламенту. Процедура, передбачена в главі VI Регламенту (ЄС) 2019/1020, застосовується mutatis mutandis.

Стаття 76

Нагляд органів ринкового нагляду за тестуванням у реальних умовах

1. Органи ринкового нагляду мають компетенції та повноваження для забезпечення відповідності тестування в реальних умовах цьому Регламенту.

2. Якщо тестування в реальних умовах проводиться для систем штучного інтелекту, що знаходяться під наглядом у рамках регуляторної пісочниці зі штучного інтелекту відповідно до статті 58, органи ринкового нагляду перевіряють відповідність статті 60 в рамках своєї наглядової ролі щодо регуляторної пісочниці зі штучного інтелекту. Ці органи можуть за потреби дозволяти проведення тестування в реальних умовах постачальником або потенційним постачальником, відступаючи від умов, встановлених у статті 60(4), пунктах (е) та (є).

3. Якщо орган ринкового нагляду отримав від потенційного постачальника, постачальника або будь-якої третьої сторони повідомлення про серйозний інцидент або має інші підстави вважати, що умови, встановлені в статтях 60 та 61, не виконуються, він може прийняти одне з таких рішень на своїй території за потреби:

(а) призупинити або припинити тестування в реальних умовах;

(б) вимагати від постачальника або потенційного постачальника та суб'єкта розгортання або потенційного суб'єкта розгортання змінити будь-який аспект тестування в реальних умовах.

4. Якщо орган ринкового нагляду прийняв рішення, зазначене в пункті 3 цієї статті, або висунув заперечення в розумінні статті 60(4), пункту (б), рішення або заперечення містить обґрунтування та роз'яснення щодо того, яким чином постачальник або потенційний постачальник може оскаржити рішення або заперечення.

5. Де це застосовно, якщо орган ринкового нагляду прийняв рішення, зазначене в пункті 3, він повідомляє його обґрунтування органам ринкового нагляду інших держав-членів, в яких систему штучного інтелекту тестували відповідно до плану тестування.

Стаття 77

Повноваження органів, що захищають основоположні права

1. Національні органи публічної влади або установи, що здійснюють нагляд або застосовують дотримання зобов'язань відповідно до права Союзу про захист основоположних прав, включаючи право на недискримінацію, стосовно використання високоризикових систем штучного інтелекту, зазначених у Додатку III, мають повноваження вимагати та отримувати доступ до будь-якої документації, створеної або збереженої відповідно до цього Регламенту, у доступній мові та форматі, коли доступ до такої документації є необхідним для ефективного виконання їхніх мандатів у межах їхньої юрисдикції. Відповідний орган публічної влади або установа інформує орган ринкового нагляду відповідної держави-члена про кожний такий запит.

2. До 2 листопада 2024 року кожна держава-член визначає органи публічної влади або установи, зазначені в пункті 1, та робить їхній перелік загальнодоступним. Держави-члени повідомляють перелік Комісії та іншим державам-членам і підтримують перелік в актуальному стані.

3. Якщо документації, зазначеної в пункті 1, недостатньо для встановлення того, чи мало місце порушення зобов'язань відповідно до права Союзу про захист основоположних прав, орган публічної влади або установа, зазначені в пункті 1, можуть подати мотивований запит до органу ринкового нагляду щодо організації тестування високоризикової системи штучного інтелекту технічними засобами. Орган ринкового нагляду організовує тестування за активної участі органу публічної влади або установи, що подала запит, у розумні строки після запиту.

4. Будь-яка інформація або документація, отримана національними органами публічної влади або установами, зазначеними в пункті 1 цієї статті відповідно до цієї статті, обробляється відповідно до зобов'язань щодо конфіденційності, встановлених у статті 78.

Стаття 78

Конфіденційність

1. Комісія, органи ринкового нагляду та нотифіковані органи і будь-яка інша фізична або юридична особа, залучена до застосування цього Регламенту, відповідно до права Союзу або національного права поважають конфіденційність інформації та даних, отриманих при виконанні своїх завдань та провадженні діяльності, таким чином, щоб захистити зокрема:

(а) права інтелектуальної власності та конфіденційну ділову інформацію або комерційні таємниці фізичної або юридичної особи, включаючи вихідний код, за винятком випадків, зазначених у статті 5 Директиви (ЄС) 2016/943 Європейського Парламенту та Ради (57);

(б) ефективну реалізацію цього Регламенту, зокрема для цілей перевірок, розслідувань або аудитів;

(в) інтереси публічної та національної безпеки;

(г) провадження кримінальних або адміністративних проваджень;

(д) інформацію, що є таємною відповідно до права Союзу або національного права.

2. Органи, залучені до застосування цього Регламенту відповідно до пункту 1, запитують лише дані, що є суворо необхідними для оцінки ризику, що становлять системи штучного інтелекту, і для здійснення своїх повноважень відповідно до цього Регламенту та Регламенту (ЄС) 2019/1020. Вони запроваджують належні та ефективні заходи кібербезпеки для захисту безпеки та конфіденційності отриманої інформації та даних і видаляють зібрані дані, як тільки вони більше не потрібні для цілей, для яких вони були отримані, відповідно до застосовного права Союзу або національного права.

3. Без шкоди для пунктів 1 та 2, інформація, якою обмінюються на конфіденційній основі між національними компетентними органами або між національними компетентними органами та Комісією, не розкривається без попередньої консультації з відповідним національним компетентним органом і суб'єктом розгортання, якщо високоризикові системи штучного інтелекту, зазначені в пунктах 1, 6 або 7 Додатку III, використовуються правоохоронними органами, органами прикордонного контролю, імміграційними або органами у справах надання притулку, і якщо таке розкриття поставить під загрозу інтереси публічної та національної безпеки. Цей обмін інформацією не охоплює чутливі оперативні дані стосовно діяльності правоохоронних органів, органів прикордонного контролю, імміграційних або органів у справах надання притулку.

Якщо правоохоронні органи, імміграційні або органи у справах надання притулку є постачальниками високоризикових систем штучного інтелекту, зазначених у пунктах 1, 6 або 7 Додатку III, технічна документація, зазначена в Додатку IV, залишається в приміщеннях цих органів. Ці органи

забезпечують, щоб органи ринкового нагляду, зазначені в статті 74(8) та (9), де це застосовно, могли на запит негайно отримати доступ до документації або отримати її копію. Лише персонал органу ринкового нагляду, що має відповідний рівень допуску до таємної інформації, має право доступу до такої документації або будь-якої її копії.

4. Пункти 1, 2 та 3 не впливають на права або зобов'язання Комісії, держав-членів та їхніх відповідних органів, а також нотифікованих органів щодо обміну інформацією та поширення попереджень, у тому числі в контексті транскордонної співпраці, а також не впливають на зобов'язання відповідних сторін надавати інформацію відповідно до кримінального законодавства держав-членів.

5. Комісія та держави-члени можуть обмінюватися за необхідності та відповідно до відповідних положень міжнародних та торговельних угод конфіденційною інформацією з регуляторними органами третіх країн, з якими вони уклали двосторонні або багатосторонні домовленості про конфіденційність, що гарантують належний рівень конфіденційності.

Стаття 79

Процедура на національному рівні щодо систем штучного інтелекту, що становлять ризик

1. Системи штучного інтелекту, що становлять ризик, розуміються як «продукт, що становить ризик», як визначено в статті 3, пункті 19 Регламенту (ЄС) 2019/1020, тією мірою, якою вони становлять ризики для здоров'я або безпеки, або для основоположних прав осіб.

2. Якщо орган ринкового нагляду держави-члена має достатні підстави вважати, що система штучного інтелекту становить ризик, як зазначено в пункті 1 цієї статті, він проводить оцінку відповідної системи штучного інтелекту стосовно її відповідності всім вимогам і зобов'язанням, встановленим у цьому Регламенті. Особлива увага приділяється системам штучного інтелекту, що становлять ризик для вразливих груп. Якщо виявляються ризики для основоположних прав, орган ринкового нагляду також інформує та повністю співпрацює з відповідними національними органами публічної влади або установами, зазначеними в статті 77(1). Відповідні оператори співпрацюють за необхідності з органом ринкового нагляду та з іншими національними органами публічної влади або установами, зазначеними в статті 77(1).

Якщо в ході такої оцінки орган ринкового нагляду або, де це застосовно, орган ринкового нагляду у співпраці з національним органом публічної влади, зазначеним у статті 77(1), встановлює, що система штучного інтелекту не відповідає вимогам та зобов'язанням, встановленим у цьому Регламенті, він без зайвих зволікань вимагає від відповідного оператора вжити всіх відповідних коригувальних заходів для приведення системи штучного інтелекту у відповідність, виведення системи штучного інтелекту з ринку або її відкликання у строк, що може бути встановлений органом ринкового нагляду, і в будь-якому випадку протягом меншого з 15 робочих днів або як передбачено у відповідному законодавстві Союзу про гармонізацію.

Орган ринкового нагляду відповідно інформує відповідний нотифікований орган. Стаття 18 Регламенту (ЄС) 2019/1020 застосовується до заходів, зазначених у другому підпункті цього пункту.

3. Якщо орган ринкового нагляду вважає, що невідповідність не обмежується його національною територією, він без зайвих зволікань інформує Комісію та інші держави-члени про результати оцінки та дії, які він вимагав від оператора вжити.

4. Оператор забезпечує вжиття всіх відповідних коригувальних заходів стосовно всіх відповідних систем штучного інтелекту, які він зробив доступними на ринку Союзу.

5. Якщо оператор системи штучного інтелекту не вживає належних коригувальних заходів протягом строку, зазначеного в пункті 2, орган ринкового нагляду вживає всіх відповідних тимчасових заходів для заборони або обмеження надання системи штучного інтелекту в розпорядження на своєму національному ринку або введення її в експлуатацію, виведення продукту або автономної системи штучного інтелекту з цього ринку або її відкликання. Цей орган без зайвих зволікань повідомляє Комісію та інші держави-члени про ці заходи.

6. Повідомлення, зазначене в пункті 5, включає всі наявні деталі, зокрема інформацію, необхідну для ідентифікації невідповідної системи штучного інтелекту, походження системи штучного інтелекту та ланцюга постачання, характер передбачуваної невідповідності та пов'язаний ризик, характер та тривалість вжитих національних заходів і аргументи, висунуті відповідним оператором. Зокрема, органи ринкового нагляду зазначають, чи є невідповідність наслідком однієї або кількох з таких причин:

(а) невідповідність забороні практик штучного інтелекту, зазначених у статті 5;

(б) недотримання високоризиковою системою штучного інтелекту вимог, встановлених у главі III, розділ 2;

(в) недоліки в гармонізованих стандартах або спільних специфікаціях, зазначених у статтях 40 та 41, що надають презумпцію відповідності;

(г) невідповідність статті 50.

7. Органи ринкового нагляду, відмінні від органу ринкового нагляду держави-члена, що ініціює процедуру, без зайвих зволікань інформують Комісію та інші держави-члени про будь-які вжиті заходи та будь-яку додаткову інформацію, що є в їхньому розпорядженні стосовно невідповідності відповідної системи штучного інтелекту, і у разі незгоди з повідомленим національним заходом — про свої заперечення.

8. Якщо протягом трьох місяців з дати отримання повідомлення, зазначеного в пункті 5 цієї статті, жодного заперечення не було висунуто ні органом ринкового нагляду держави-члена, ні Комісією стосовно тимчасового заходу, вжитого органом ринкового нагляду іншої держави-члена, такий захід вважається обґрунтованим. Це не завдає шкоди процесуальним правам відповідного оператора відповідно до статті 18 Регламенту (ЄС) 2019/1020. Тримісячний строк, зазначений у цьому пункті, скорочується до 30 днів у разі невідповідності забороні практик штучного інтелекту, зазначених у статті 5 цього Регламенту.

9. Органи ринкового нагляду забезпечують вжиття відповідних обмежувальних заходів стосовно відповідного продукту або системи штучного інтелекту, таких як виведення продукту або системи штучного інтелекту з їхнього ринку, без зайвих зволікань.

Стаття 80

Процедура щодо систем штучного інтелекту, класифікованих постачальником як не-високоризикові при застосуванні Додатку III

1. Якщо орган ринкового нагляду має достатні підстави вважати, що система штучного інтелекту, класифікована постачальником як не-високоризикова відповідно до статті 6(3), є насправді високоризиковою, орган ринкового нагляду проводить оцінку відповідної системи штучного інтелекту стосовно її класифікації як високоризикової системи штучного інтелекту на підставі умов, встановлених у статті 6(3) та настановах Комісії.

2. Якщо в ході такої оцінки орган ринкового нагляду встановлює, що відповідна система штучного інтелекту є високоризиковою, він без зайвих зволікань вимагає від відповідного постачальника вжити всіх необхідних заходів для приведення системи штучного інтелекту у відповідність вимогам і зобов'язанням, встановленим у цьому Регламенті, а також вжити відповідних коригувальних заходів протягом строку, що може бути встановлений органом ринкового нагляду.

3. Якщо орган ринкового нагляду вважає, що використання відповідної системи штучного інтелекту не обмежується його національною територією, він без зайвих зволікань інформує Комісію та інші держави-члени про результати оцінки та дії, які він вимагав від постачальника вжити.

4. Постачальник забезпечує вжиття всіх необхідних заходів для приведення системи штучного інтелекту у відповідність вимогам та зобов'язанням, встановленим у цьому Регламенті. Якщо постачальник відповідної системи штучного інтелекту не приводить систему штучного інтелекту у відповідність цим вимогам та зобов'язанням протягом строку, зазначеного в пункті 2 цієї статті, постачальник підлягає штрафам відповідно до статті 99.

5. Постачальник забезпечує вжиття всіх відповідних коригувальних заходів стосовно всіх відповідних систем штучного інтелекту, які він зробив доступними на ринку Союзу.

6. Якщо постачальник відповідної системи штучного інтелекту не вживає належних коригувальних заходів протягом строку, зазначеного в пункті 2 цієї статті, застосовуються статті 79(5)–(9).

7. Якщо в ході оцінки відповідно до пункту 1 цієї статті орган ринкового нагляду встановлює, що система штучного інтелекту була помилково класифікована постачальником як не-високоризикова з метою обходу застосування вимог у главі III, розділ 2, постачальник підлягає штрафам відповідно до статті 99.

8. При здійсненні своїх повноважень з моніторингу застосування цієї статті та відповідно до статті 11 Регламенту (ЄС) 2019/1020 органи ринкового нагляду можуть проводити відповідні перевірки, беручи до уваги зокрема інформацію, що зберігається в базі даних ЄС, зазначеній у статті 71 цього Регламенту.

Стаття 81

Захисна процедура Союзу

1. Якщо протягом трьох місяців з дати отримання повідомлення, зазначеного в статті 79(5), або протягом 30 днів у разі невідповідності забороні практик штучного інтелекту, зазначених у статті 5, органом ринкового нагляду держави-члена висуваються заперечення щодо заходу, вжитого іншим органом ринкового нагляду, або якщо Комісія вважає захід таким, що суперечить праву Союзу, Комісія без зайвих зволікань вступає в консультації з органом ринкового нагляду відповідної держави-члена та оператором або операторами і оцінює національний захід. На підставі результатів такої оцінки Комісія протягом шести місяців або протягом 60 днів у разі невідповідності забороні практик штучного інтелекту, зазначених у статті 5, починаючи з повідомлення, зазначеного в статті 79(5), приймає рішення про те, чи є національний захід обґрунтованим, і повідомляє своє рішення органу ринкового нагляду відповідної держави-члена. Комісія також інформує всі інші органи ринкового нагляду про своє рішення.

2. Якщо Комісія вважає захід, вжитий відповідною державою-членом, обґрунтованим, всі держави-члени забезпечують вжиття відповідних обмежувальних заходів стосовно відповідної системи штучного інтелекту, таких як вимога виведення системи штучного інтелекту з їхнього ринку без зайвих зволікань, та відповідно інформують Комісію. Якщо Комісія вважає національний захід необґрунтованим, відповідна держава-член скасовує захід та відповідно інформує Комісію.

3. Якщо національний захід вважається обґрунтованим і невідповідність системи штучного інтелекту пов'язана з недоліками в гармонізованих стандартах або спільних специфікаціях, зазначених у статтях 40 та 41 цього Регламенту, Комісія застосовує процедуру, передбачену в статті 11 Регламенту (ЄС) № 1025/2012.

Стаття 82

Відповідні системи штучного інтелекту, що становлять ризик

1. Якщо, провівши оцінку відповідно до статті 79, після консультації з відповідним національним органом публічної влади, зазначеним у статті 77(1), орган ринкового нагляду держави-члена встановлює, що хоча високоризикова система штучного інтелекту відповідає цьому Регламенту, вона, тим не менш, становить ризик для здоров'я або безпеки осіб, основоположних прав або інших аспектів захисту суспільних інтересів, він вимагає від відповідного оператора вжити всіх відповідних заходів для забезпечення того, щоб відповідна система штучного інтелекту, будучи введеною в обіг або введеною в експлуатацію, більше не становила цього ризику без зайвих зволікань, у строк, що він може встановити.

2. Постачальник або інший відповідний оператор забезпечує вжиття коригувальних заходів стосовно всіх відповідних систем штучного інтелекту, які він зробив доступними на ринку Союзу, у строк, визначений органом ринкового нагляду держави-члена, зазначеним у пункті 1.

3. Держави-члени негайно інформують Комісію та інші держави-члени про висновок відповідно до пункту 1. Така інформація включає всі наявні деталі, зокрема дані, необхідні для ідентифікації відповідної системи штучного інтелекту, походження та ланцюга постачання системи штучного інтелекту, характер пов'язаного ризику та характер і тривалість вжитих національних заходів.

4. Комісія без зайвих зволікань вступає в консультації з відповідними державами-членами та відповідними операторами та оцінює вжиті національні заходи. На підставі результатів такої оцінки Комісія приймає рішення про те, чи є захід обґрунтованим, і за необхідності пропонує інші відповідні заходи.

5. Комісія негайно повідомляє своє рішення відповідним державам-членам та відповідним операторам. Вона також інформує інші держави-члени.

Стаття 83

Формальна невідповідність

1. Якщо орган ринкового нагляду держави-члена робить один з таких висновків, він вимагає від відповідного постачальника покласти край відповідній невідповідності у строк, що він може встановити:

(a) маркування CE було нанесено з порушенням статті 48;

(б)	маркування CE не було нанесено;
(в)	декларація відповідності ЄС, зазначена в статті 47, не була складена;
(г)	декларація відповідності ЄС, зазначена в статті 47, не була складена правильно;
(д)	реєстрація в базі даних ЄС, зазначеній у статті 71, не була проведена;
(е)	де це застосовно, жодного уповноваженого представника не було призначено;
(є)	технічна документація недоступна.

2. Якщо невідповідність, зазначена в пункті 1, зберігається, орган ринкового нагляду відповідної держави-члена вживає відповідних і пропорційних заходів для обмеження або заборони надання высокоризикової системи штучного інтелекту в розпорядження на ринку або для забезпечення її відкликання або виведення з ринку без зволікань.

Стаття 84

Структури підтримки тестування штучного інтелекту Союзу

1. Комісія призначає одну або кілька структур підтримки тестування штучного інтелекту Союзу для виконання завдань, перелічених у статті 21(6) Регламенту (ЄС) 2019/1020, у сфері штучного інтелекту.

2. Без шкоди для завдань, зазначених у пункті 1, структури підтримки тестування штучного інтелекту Союзу також надають незалежні технічні або наукові консультації на запит Ради, Комісії або органів ринкового нагляду.

РОЗДІЛ 4

Засоби правового захисту

Стаття 85

Право на подання скарги до органу ринкового нагляду

Без шкоди для інших адміністративних або судових засобів правового захисту, будь-яка фізична або юридична особа, яка має підстави вважати, що мало місце порушення положень цього Регламенту, може подавати скарги до відповідного органу ринкового нагляду.

Відповідно до Регламенту (ЄС) 2019/1020, такі скарги беруться до уваги для цілей здійснення діяльності з ринкового нагляду і розглядаються відповідно до спеціальних процедур, встановлених для цього органами ринкового нагляду.

Стаття 86

Право на пояснення при прийнятті індивідуальних рішень

1. Будь-яка постраждала особа, щодо якої суб'єкт розгортання прийняв рішення на підставі результатів роботи високоризикової системи штучного інтелекту, переліченої в Додатку III, за винятком систем, перелічених у пункті 2 цього додатку, і яке породжує правові наслідки або подібним чином суттєво впливає на цю особу в спосіб, що, на її думку, негативно впливає на її здоров'я, безпеку або основоположні права, має право отримати від суб'єкта розгортання чіткі та зрозумілі пояснення ролі системи штучного інтелекту в процедурі прийняття рішень та основних елементів прийнятого рішення.

2. Пункт 1 не застосовується до використання систем штучного інтелекту, щодо яких винятки із зобов'язання відповідно до цього пункту або обмеження такого зобов'язання випливають із права Союзу або національного права відповідно до права Союзу.

3. Ця стаття застосовується лише тою мірою, якою право, зазначене в пункті 1, не передбачено в інший спосіб відповідно до права Союзу.

Стаття 87

Повідомлення про порушення та захист осіб, що повідомляють

Директива (ЄС) 2019/1937 застосовується до повідомлення про порушення цього Регламенту та захисту осіб, що повідомляють про такі порушення.

РОЗДІЛ 5

Нагляд, розслідування, застосування та моніторинг стосовно постачальників моделей штучного інтелекту загального призначення

Стаття 88

Застосування зобов'язань постачальників моделей штучного інтелекту загального призначення

1. Комісія має виключні повноваження з нагляду та застосування глави V з урахуванням процесуальних гарантій відповідно до статті 94. Комісія доручає реалізацію цих завдань Офісу зі штучного інтелекту без шкоди для організаційних повноважень Комісії та розподілу компетенцій між державами-членами та Союзом на підставі Договорів.

2. Без шкоди для статті 75(3) органи ринкового нагляду можуть звертатися до Комісії з проханням здійснити повноваження, встановлені в цьому розділі, якщо це є необхідним і пропорційним для сприяння виконанню їхніх завдань відповідно до цього Регламенту.

Стаття 89

Дії з моніторингу

1. Для цілей виконання завдань, покладених на нього в рамках цього розділу, Офіс зі штучного інтелекту може вживати необхідних заходів для моніторингу ефективної реалізації та дотримання цього Регламенту постачальниками моделей штучного інтелекту загального призначення, включаючи їхнє дотримання затверджених кодексів поведінки.

2. Постачальники нижчої ланки мають право подати скаргу із зазначенням передбачуваного порушення цього Регламенту. Скарга повинна бути належним чином обґрунтована та вказувати щонайменше:

(а)	контактну точку постачальника відповідної моделі штучного інтелекту загального призначення;
(б)	опис відповідних фактів, положень цього Регламенту, яких вони стосуються, та причини, з яких постачальник нижчої ланки вважає, що постачальник відповідної моделі штучного інтелекту загального призначення порушив цей Регламент;
(в)	будь-яку іншу інформацію, яку постачальник нижчої ланки, що надіслав запит, вважає релевантною, включаючи за потреби інформацію, зібрану за власною ініціативою.

Стаття 90

Оповіщення про системні ризики науковою радою

1. Наукова рада може направляти кваліфіковане оповіщення до Офісу зі штучного інтелекту, якщо має підстави підозрювати, що:

(а) модель штучного інтелекту загального призначення становить конкретний ідентифікований ризик на рівні Союзу; або

(б) модель штучного інтелекту загального призначення відповідає умовам, зазначеним у статті 51.

2. На таке кваліфіковане оповіщення Комісія через Офіс зі штучного інтелекту та після інформування Ради може здійснювати повноваження, встановлені в цьому розділі, з метою оцінки питання. Офіс зі штучного інтелекту інформує Раду про будь-який захід відповідно до статей 91–94.

3. Кваліфіковане оповіщення повинно бути належним чином обґрунтоване та вказувати щонайменше:

(а) контактну точку постачальника відповідної моделі штучного інтелекту загального призначення із системним ризиком;

(б) опис відповідних фактів та причин оповіщення науковою радою;

(в) будь-яку іншу інформацію, яку наукова рада вважає релевантною, включаючи за потреби інформацію, зібрану за власною ініціативою.

Стаття 91

Повноваження щодо запиту документації та інформації

1. Комісія може звернутися до постачальника відповідної моделі штучного інтелекту загального призначення з проханням надати документацію, складену постачальником відповідно до статей 53 та 55, або будь-яку додаткову інформацію, необхідну для цілей оцінки відповідності постачальника вимогам цього Регламенту.

2. Перед надсиланням запиту на інформацію Офіс зі штучного інтелекту може ініціювати структурований діалог з постачальником моделі штучного інтелекту загального призначення.

3. На обґрунтований запит наукової ради Комісія може надіслати запит на інформацію до постачальника моделі штучного інтелекту загального призначення, якщо доступ до інформації є необхідним і пропорційним для виконання завдань наукової ради відповідно до статті 68(2).

4. Запит на інформацію повинен містити правову підставу та мету запиту, визначати, яка інформація вимагається, встановлювати строк, протягом якого має бути надана інформація, та вказувати штрафи, передбачені в статті 101 за надання неправильної, неповної або оманливої інформації.

5. Постачальник відповідної моделі штучного інтелекту загального призначення або його представник надає запитану інформацію. У разі юридичних осіб, компаній або фірм, або якщо постачальник не має статусу юридичної особи, особи, уповноважені представляти їх за законом або їхніми статутами, надають запитану інформацію від імені постачальника відповідної моделі штучного

інтелекту загального призначення. Юристи, належним чином уповноважені діяти, можуть надавати інформацію від імені своїх клієнтів. Клієнти, проте, несуть повну відповідальність, якщо надана інформація є неповною, неправильною або оманливою.

Стаття 92

Повноваження щодо проведення оцінок

1. Офіс зі штучного інтелекту після консультації з Радою може проводити оцінки відповідної моделі штучного інтелекту загального призначення:

(а) для оцінки відповідності постачальника зобов'язанням відповідно до цього Регламенту, якщо інформація, зібрана відповідно до статті 91, є недостатньою; або

(б) для дослідження системних ризиків на рівні Союзу з боку моделей штучного інтелекту загального призначення із системним ризиком, зокрема після кваліфікованого оповіщення від наукової ради відповідно до статті 90(1), пункту (а).

2. Комісія може ухвалити рішення про призначення незалежних експертів для проведення оцінок від її імені, у тому числі з наукової ради, створеної відповідно до статті 68. Незалежні експерти, призначені для цього завдання, повинні відповідати критеріям, визначеним у статті 68(2).

3. Для цілей пункту 1 Комісія може запитати доступ до відповідної моделі штучного інтелекту загального призначення через API або інші відповідні технічні засоби та інструменти, включаючи вихідний код.

4. Запит на доступ повинен містити правову підставу, мету та причини запиту, встановлювати строк, протягом якого має бути надано доступ, та штрафи, передбачені в статті 101 за ненадання доступу.

5. Постачальники відповідної моделі штучного інтелекту загального призначення або її представник надають запитану інформацію. У разі юридичних осіб, компаній або фірм, або якщо постачальник не має статусу юридичної особи, особи, уповноважені представляти їх за законом або їхніми статутами, надають запитаний доступ від імені постачальника відповідної моделі штучного інтелекту загального призначення.

6. Комісія ухвалює імплементаційні акти, що встановлюють детальні правила та умови проведення оцінок, включаючи детальні правила щодо залучення незалежних експертів та процедуру їх відбору. Ці імплементаційні акти ухвалюються відповідно до процедури розгляду, зазначеної в статті 98(2).

7. До подання запиту на доступ до відповідної моделі штучного інтелекту загального призначення Офіс зі штучного інтелекту може ініціювати структурований діалог з постачальником моделі штучного інтелекту загального призначення для збору додаткової інформації про внутрішнє тестування моделі, внутрішні засоби захисту від системних ризиків та інші внутрішні процедури та заходи, вжиті постачальником для зменшення таких ризиків.

Стаття 93

Повноваження щодо запиту заходів

1. Там, де це необхідно та доцільно, Комісія може вимагати від постачальників:

(а)	вжити відповідних заходів для виконання зобов'язань, встановлених у статтях 53 та 54;
(б)	запровадити заходи зі зменшення ризиків, якщо оцінка, проведена відповідно до статті 92, зумовила серйозні та обґрунтовані побоювання щодо системного ризику на рівні Союзу;
(в)	обмежити надання моделі в розпорядження на ринку, відкликати або вилучити модель.

2. Перед тим як вимагати заходів, Офіс зі штучного інтелекту може ініціювати структурований діалог з постачальником моделі штучного інтелекту загального призначення.

3. Якщо під час структурованого діалогу, зазначеного в пункті 2, постачальник моделі штучного інтелекту загального призначення із системним ризиком пропонує зобов'язання щодо запровадження заходів зі зменшення ризиків для усунення системного ризику на рівні Союзу, Комісія може рішенням зробити ці зобов'язання обов'язковими та оголосити, що немає подальших підстав для вжиття заходів.

Стаття 94

Процесуальні права суб'єктів господарювання щодо моделі штучного інтелекту загального призначення

Стаття 18 Регламенту (ЄС) 2019/1020 застосовується mutatis mutandis до постачальників моделі штучного інтелекту загального призначення без шкоди для більш конкретних процесуальних прав, передбачених у цьому Регламенті.

ГЛАВА X

КОДЕКСИ ПОВЕДІНКИ ТА НАСТАНОВИ

Стаття 95

Кодекси поведінки для добровільного застосування конкретних вимог

1. Офіс зі штучного інтелекту та держави-члени заохочують і сприяють розробці кодексів поведінки, включаючи пов'язані механізми управління, призначених для сприяння добровільному застосуванню до систем штучного інтелекту, окрім високоризикових систем штучного інтелекту, деяких або всіх вимог, встановлених у главі III, розділі 2, з урахуванням доступних технічних рішень та найкращих галузевих практик, що дозволяють застосовувати такі вимоги.

2. Офіс зі штучного інтелекту та держави-члени сприяють розробці кодексів поведінки щодо добровільного застосування, у тому числі суб'єктами розгортання, конкретних вимог до всіх систем штучного інтелекту на основі чітких цілей та ключових показників ефективності для вимірювання досягнення цих цілей, включаючи такі елементи, як зокрема, але не виключно:

(а) застосовні елементи, передбачені в етичних настановах Союзу для надійного штучного інтелекту;

(б) оцінку та мінімізацію впливу систем штучного інтелекту на екологічну стійкість, у тому числі щодо енергоефективного програмування та методів ефективного проектування, навчання та використання штучного інтелекту;

(в) сприяння поширенню грамотності в сфері штучного інтелекту, зокрема серед осіб, що займаються розробкою, експлуатацією та використанням штучного інтелекту;

(г) сприяння інклюзивному та різноманітному проектуванню систем штучного інтелекту, у тому числі шляхом створення інклюзивних та різноманітних груп розробників і заохочення участі зацікавлених сторін у цьому процесі;

(д) оцінку та запобігання негативному впливу систем штучного інтелекту на вразливих осіб або групи вразливих осіб, у тому числі щодо доступності для осіб з інвалідністю, а також щодо гендерної рівності.

3. Кодекси поведінки можуть розроблятися окремими постачальниками або суб'єктами розгортання систем штучного інтелекту чи організаціями, що їх представляють, або обома, у тому числі із залученням будь-яких зацікавлених сторін та їхніх представницьких організацій, включаючи

організації громадянського суспільства та академічні установи. Кодекси поведінки можуть охоплювати одну або кілька систем штучного інтелекту з урахуванням схожості передбачуваного призначення відповідних систем.

4. Офіс зі штучного інтелекту та держави-члени беруть до уваги конкретні інтереси та потреби МСП, включаючи стартапи, під час заохочення та сприяння розробці кодексів поведінки.

Стаття 96

Настанови Комісії щодо виконання цього Регламенту

1. Комісія розробляє настанови щодо практичного виконання цього Регламенту, і зокрема щодо:

(а)	застосування вимог та зобов'язань, зазначених у статтях 8–15 та в статті 25;
(б)	заборонених практик, зазначених у статті 5;
(в)	практичного виконання положень, пов'язаних із суттєвою модифікацією;
(г)	практичного виконання зобов'язань щодо прозорості, встановлених у статті 50;
(д)	детальної інформації про співвідношення цього Регламенту із законодавством Союзу про гармонізацію, переліченим у Додатку I, а також з іншим відповідним правом Союзу, у тому числі щодо узгодженості в їх застосуванні;
(е)	застосування визначення системи штучного інтелекту, встановленого в статті 3, пункті (1).

Під час видачі таких настанов Комісія приділяє особливу увагу потребам МСП, включаючи стартапи, місцевих органів публічної влади та секторів, що, найімовірніше, зазнають впливу цього Регламенту.

Настанови, зазначені в першому підпункті цього пункту, належним чином враховують загальновизнаний рівень розвитку штучного інтелекту, а також відповідні гармонізовані стандарти та спільні специфікації, зазначені в статтях 40 та 41, або ті гармонізовані стандарти чи технічні специфікації, що встановлені відповідно до законодавства Союзу про гармонізацію.

2. На запит держав-членів або Офісу зі штучного інтелекту, або з власної ініціативи Комісія оновлює раніше прийняті настанови, якщо це вважається необхідним.

ГЛАВА XI

ДЕЛЕГУВАННЯ ПОВНОВАЖЕНЬ ТА ПРОЦЕДУРА КОМІТЕТУ

Стаття 97

Здійснення делегування

1. Повноваження щодо ухвалення делегованих актів надається Комісії з дотриманням умов, встановлених у цій статті.

2. Повноваження щодо ухвалення делегованих актів, зазначених у статті 6(6) та (7), статті 7(1) та (3), статті 11(3), статті 43(5) та (6), статті 47(5), статті 51(3), статті 52(4) та статті 53(5) та (6), надається Комісії на п'ятирічний строк з 1 серпня 2024 року. Комісія складає звіт щодо делегування повноважень не пізніше ніж за дев'ять місяців до закінчення п'ятирічного строку. Делегування повноважень мовчазно продовжується на строки однакової тривалості, якщо Європейський Парламент або Рада не заперечують проти такого продовження не пізніше ніж за три місяці до закінчення кожного строку.

3. Делегування повноважень, зазначене в статті 6(6) та (7), статті 7(1) та (3), статті 11(3), статті 43(5) та (6), статті 47(5), статті 51(3), статті 52(4) та статті 53(5) та (6), може бути відкликане в будь-який час Європейським Парламентом або Радою. Рішення про відкликання припиняє делегування повноважень, визначене в цьому рішенні. Воно набирає чинності наступного дня після його публікації в Офіційному журналі Європейського Союзу або в більш пізню дату, зазначену в ньому. Воно не впливає на чинність будь-яких делегованих актів, що вже набрали чинності.

4. Перед ухваленням делегованого акта Комісія консультується з експертами, призначеними кожною державою-членом відповідно до принципів, встановлених у Міжінституційній угоді від 13 квітня 2016 року про якість законодавства.

5. Щойно Комісія ухвалює делегований акт, вона одночасно повідомляє про нього Європейський Парламент і Раду.

6. Будь-який делегований акт, ухвалений відповідно до статті 6(6) або (7), статті 7(1) або (3), статті 11(3), статті 43(5) або (6), статті 47(5), статті 51(3), статті 52(4) або статті 53(5) або (6), набирає чинності лише за умови, що ані Європейський Парламент, ані Рада не висловили заперечень протягом трьох місяців з моменту повідомлення про цей акт Європейському Парламенту та Раді, або якщо до закінчення цього строку Європейський Парламент і Рада обидва повідомили Комісію, що не будуть заперечувати. Цей строк продовжується на три місяці за ініціативою Європейського Парламенту або Ради.

Стаття 98

Процедура комітету

1. Комісії надає допомогу комітет. Цей комітет є комітетом у розумінні Регламенту (ЄС) № 182/2011.

2. У разі покликання на цей пункт застосовується стаття 5 Регламенту (ЄС) № 182/2011.

ГЛАВА XII

САНКЦІЇ

Стаття 99

Санкції

1. Відповідно до умов, встановлених у цьому Регламенті, держави-члени встановлюють правила щодо санкцій та інших заходів виконання, які можуть також включати попередження та немонетарні заходи, що застосовуються до порушень цього Регламенту операторами, та вживають усіх заходів, необхідних для забезпечення їх належного та ефективного виконання, враховуючи настанови, видані Комісією відповідно до статті 96. Передбачені санкції є ефективними, пропорційними та стримувальними. Вони враховують інтереси МСП, включаючи стартапи, та їхню економічну життєздатність.

2. Держави-члени без зволікань та не пізніше дати набрання чинності повідомляють Комісію про правила щодо санкцій та інших заходів виконання, зазначених у пункті 1, і без зволікань повідомляють її про будь-які подальші зміни до них.

3. Недотримання заборони практик штучного інтелекту, зазначених у статті 5, тягне за собою адміністративні штрафи в розмірі до 35 000 000 євро або, якщо порушник є підприємством, до 7 % його загального світового річного обороту за попередній фінансовий рік — залежно від того, яка сума є більшою.

4. Недотримання будь-якого з таких положень, що стосуються операторів або нотифікованих органів, окрім тих, що встановлені в статті 5, тягне за собою адміністративні штрафи в розмірі до 15 000 000 євро або, якщо порушник є підприємством, до 3 % його загального світового річного обороту за попередній фінансовий рік — залежно від того, яка сума є більшою:

(а)	зобов'язань постачальників відповідно до статті 16;
(б)	зобов'язань уповноважених представників відповідно до статті 22;
(в)	зобов'язань імпортерів відповідно до статті 23;
(г)	зобов'язань дистриб'юторів відповідно до статті 24;
(д)	зобов'язань суб'єктів розгортання відповідно до статті 26;
(е)	вимог та зобов'язань нотифікованих органів відповідно до статті 31, статті 33(1), (3) та (4) або статті 34;
(є)	зобов'язань постачальників і суб'єктів розгортання щодо прозорості відповідно до статті 50.

5. Надання неправильної, неповної або оманливої інформації нотифікованим органам або національним компетентним органам у відповідь на запит тягне за собою адміністративні штрафи в розмірі до 7 500 000 євро або, якщо порушник є підприємством, до 1 % його загального світового річного обороту за попередній фінансовий рік — залежно від того, яка сума є більшою.

6. У разі МСП, включаючи стартапи, кожен штраф, зазначений у цій статті, не перевищує відсотків або суми, зазначених у пунктах 3, 4 та 5, залежно від того, яка з них є меншою.

7. Вирішуючи, чи накладати адміністративний штраф, та визначаючи розмір адміністративного штрафу в кожному конкретному випадку, беруться до уваги всі відповідні обставини конкретної ситуації та, за потреби, враховується таке:

(а)	характер, тяжкість та тривалість порушення та його наслідків з урахуванням призначення системи штучного інтелекту, а також, де це доцільно, кількість постраждалих осіб та рівень шкоди, якої вони зазнали;
(б)	чи вже були накладені адміністративні штрафи іншими органами ринкового нагляду на того самого оператора за те саме порушення;
(в)	чи вже були накладені адміністративні штрафи іншими органами на того самого оператора за порушення іншого права Союзу або національного права, якщо такі порушення є наслідком тієї самої діяльності або бездіяльності, що складає відповідне порушення цього Регламенту;
(г)	розмір, річний оборот та частку ринку оператора, що вчинив порушення;
(д)	будь-які інші обтяжуючі або пом'якшуючі обставини, застосовні до обставин справи, такі як фінансова вигода, отримана, або збитки, уникнуті, прямо або опосередковано, внаслідок порушення;
(е)	ступінь співпраці з національними компетентними органами з метою усунення порушення та зменшення можливих негативних наслідків порушення;
(є)	ступінь відповідальності оператора з урахуванням технічних та організаційних заходів, що він вжив;
(ж)	спосіб, у який порушення стало відомим національним компетентним органам, зокрема чи і якою мірою оператор повідомив про

порушення;

(з) навмисний або необережний характер порушення;

(и) будь-які заходи, вжиті оператором для зменшення шкоди, якої зазнали постраждалі особи.

8. Кожна держава-член встановлює правила щодо того, якою мірою адміністративні штрафи можуть накладатися на органи публічної влади та установи, створені в цій державі-члені.

9. Залежно від правової системи держав-членів, правила щодо адміністративних штрафів можуть застосовуватися таким чином, щоб штрафи накладалися компетентними національними судами або іншими органами, що застосовуються в цих державах-членах. Застосування таких правил у цих державах-членах має рівнозначний ефект.

10. Здійснення повноважень відповідно до цієї статті підпорядковується відповідним процесуальним гарантіям відповідно до права Союзу та національного права, включаючи ефективні засоби судового захисту та належний судовий процес.

11. Держави-члени на щорічній основі звітують Комісії про адміністративні штрафи, які вони наклали протягом цього року відповідно до цієї статті, та про будь-які пов'язані судові спори або судові провадження.

Стаття 100

Адміністративні штрафи для інституцій, органів, служб та агентств Союзу

1. Європейський інспектор із захисту даних може накладати адміністративні штрафи на інституції, органи, служби та агентства Союзу, що підпадають під сферу дії цього Регламенту. Вирішуючи, чи накладати адміністративний штраф, та визначаючи розмір адміністративного штрафу в кожному конкретному випадку, беруться до уваги всі відповідні обставини конкретної ситуації та належно враховується таке:

(а) характер, тяжкість та тривалість порушення та його наслідків з урахуванням призначення відповідної системи штучного інтелекту, а також, де це доцільно, кількість постраждалих осіб та рівень шкоди, якої вони зазнали;

(б) ступінь відповідальності інституції, органу, служби або агентства Союзу з урахуванням технічних та організаційних заходів, що ними вжиті;

(в) будь-які заходи, вжиті інституцією, органом, службою або агентством Союзу для зменшення шкоди, якої зазнали постраждалі особи;

(г)	ступінь співпраці з Європейським інспектором із захисту даних з метою усунення порушення та зменшення можливих негативних наслідків порушення, включаючи дотримання будь-яких заходів, раніше приписаних Європейським інспектором із захисту даних щодо відповідної інституції, органу, служби або агентства Союзу стосовно тієї самої предметної сфери;
(д)	будь-які аналогічні попередні порушення з боку інституції, органу, служби або агентства Союзу;
(е)	спосіб, у який порушення стало відомим Європейському інспектору із захисту даних, зокрема чи і якою мірою інституція, орган, служба або агентство Союзу повідомили про порушення;
(є)	річний бюджет інституції, органу, служби або агентства Союзу.

2. Недотримання заборони практик штучного інтелекту, зазначених у статті 5, тягне за собою адміністративні штрафи в розмірі до 1 500 000 євро.

3. Невідповідність системи штучного інтелекту будь-яким вимогам або зобов'язанням відповідно до цього Регламенту, окрім тих, що встановлені в статті 5, тягне за собою адміністративні штрафи в розмірі до 750 000 євро.

4. До прийняття рішень відповідно до цієї статті Європейський інспектор із захисту даних надає інституції, органу, службі або агентству Союзу, що є предметом провадження, яке здійснює Європейський інспектор із захисту даних, можливість бути заслуханими з питань щодо можливого порушення. Європейський інспектор із захисту даних ґрунтує свої рішення лише на елементах та обставинах, щодо яких відповідні сторони мали змогу висловитися. Скаржники, якщо такі є, тісно пов'язуються з провадженням.

5. Права на захист відповідних сторін повністю поважаються в ході провадження. Вони мають право на доступ до матеріалів справи Європейського інспектора із захисту даних з урахуванням законних інтересів фізичних осіб або підприємств у захисті їхніх персональних даних або комерційних таємниць.

6. Кошти, зібрані шляхом накладення штрафів відповідно до цієї статті, надходять до загального бюджету Союзу. Штрафи не повинні впливати на ефективне функціонування інституції, органу, служби або агентства Союзу, на яких накладено штраф.

7. Європейський інспектор із захисту даних на щорічній основі повідомляє Комісії про адміністративні штрафи, які він наклав відповідно до цієї статті, та про будь-які судові спори або судові провадження, які він ініціював.

Стаття 101

Штрафи для постачальників моделей штучного інтелекту загального призначення

1. Комісія може накладати на постачальників моделей штучного інтелекту загального призначення штрафи, що не перевищують 3 % їхнього загального річного світового обороту за попередній фінансовий рік або 15 000 000 євро — залежно від того, яка сума є більшою, — якщо Комісія встановлює, що постачальник навмисно або з необережності:

(а) порушив відповідні положення цього Регламенту;

(б) не виконав запит щодо документа або інформації відповідно до статті 91 або надав неправильну, неповну або оманливу інформацію;

(в) не виконав захід, запитаний відповідно до статті 93;

(г) не надав Комісії доступ до моделі штучного інтелекту загального призначення або моделі штучного інтелекту загального призначення із системним ризиком з метою проведення оцінки відповідно до статті 92.

При визначенні розміру штрафу або регулярних виплат за примусом враховуються характер, тяжкість та тривалість порушення з належним урахуванням принципів пропорційності та доцільності. Комісія також враховує зобов'язання, взяті відповідно до статті 93(3) або взяті у відповідних кодексах поведінки відповідно до статті 56.

2. Перед ухваленням рішення відповідно до пункту 1 Комісія повідомляє постачальника моделі штучного інтелекту загального призначення про свої попередні висновки та надає йому можливість бути заслуханим.

3. Штрафи, накладені відповідно до цієї статті, є ефективними, пропорційними та стримувальними.

4. Інформація про штрафи, накладені відповідно до цієї статті, також за потреби повідомляється Раді.

5. Суд справедливості Європейського Союзу має необмежену юрисдикцію для перегляду рішень Комісії про встановлення штрафу відповідно до цієї статті. Він може скасувати, зменшити або збільшити накладений штраф.

6. Комісія ухвалює імплементаційні акти, що містять детальні правила та процесуальні гарантії для проваджень, що мають на меті можливе ухвалення рішень відповідно до пункту 1 цієї статті. Ці імплементаційні акти ухвалюються відповідно до процедури розгляду, зазначеної в статті 98(2).

ГЛАВА XIII

ПРИКІНЦЕВІ ПОЛОЖЕННЯ

Стаття 102

Внесення змін до Регламенту (ЄС) № 300/2008

До статті 4(3) Регламенту (ЄС) № 300/2008 додається такий підпункт:

'При ухваленні детальних заходів, пов'язаних із технічними специфікаціями та процедурами затвердження та використання обладнання безпеки, що стосується систем штучного інтелекту в розумінні Регламенту (ЄС) 2024/1689 Європейського Парламенту та Ради (*), враховуються вимоги, встановлені в главі III, розділі 2, цього Регламенту.

Стаття 103

Внесення змін до Регламенту (ЄС) № 167/2013

До статті 17(5) Регламенту (ЄС) № 167/2013 додається такий підпункт:

'При ухваленні делегованих актів відповідно до першого підпункту, що стосуються систем штучного інтелекту, які є компонентами безпеки в розумінні Регламенту (ЄС) 2024/1689 Європейського Парламенту та Ради (*), враховуються вимоги, встановлені в главі III, розділі 2, цього Регламенту.

Стаття 104

Внесення змін до Регламенту (ЄС) № 168/2013

До статті 22(5) Регламенту (ЄС) № 168/2013 додається такий підпункт:

'При ухваленні делегованих актів відповідно до першого підпункту, що стосуються систем штучного інтелекту, які є компонентами безпеки в розумінні Регламенту (ЄС) 2024/1689 Європейського Парламенту та Ради (*), враховуються вимоги, встановлені в главі III, розділі 2, цього Регламенту.

Стаття 105

Внесення змін до Директиви 2014/90/ЄС

До статті 8 Директиви 2014/90/ЄС додається такий пункт:

'5. Щодо систем штучного інтелекту, які є компонентами безпеки в розумінні Регламенту (ЄС) 2024/1689 Європейського Парламенту та Ради (*), при здійсненні своєї діяльності відповідно до пункту 1 та при ухваленні технічних специфікацій і стандартів тестування відповідно до пунктів 2 та 3, Комісія враховує вимоги, встановлені в главі III, розділі 2, цього Регламенту.

Стаття 106

Внесення змін до Директиви (ЄС) 2016/797

До статті 5 Директиви (ЄС) 2016/797 додається такий пункт:

'12. При ухваленні делегованих актів відповідно до пункту 1 та імплементаційних актів відповідно до пункту 11, що стосуються систем штучного інтелекту, які є компонентами безпеки в розумінні Регламенту (ЄС) 2024/1689 Європейського Парламенту та Ради (*), враховуються вимоги, встановлені в главі III, розділі 2, цього Регламенту.

Стаття 107

Внесення змін до Регламенту (ЄС) 2018/858

До статті 5 Регламенту (ЄС) 2018/858 додається такий пункт:

'4. При ухваленні делегованих актів відповідно до пункту 3, що стосуються систем штучного інтелекту, які є компонентами безпеки в розумінні Регламенту (ЄС) 2024/1689 Європейського Парламенту та Ради (*), враховуються вимоги, встановлені в главі III, розділі 2, цього Регламенту.

Стаття 108

Внесення змін до Регламенту (ЄС) 2018/1139

До Регламенту (ЄС) 2018/1139 вносяться такі зміни:

(1) до статті 17 додається такий пункт:

'3. Без шкоди для пункту 2, при ухваленні імплементаційних актів відповідно до пункту 1, що стосуються систем штучного інтелекту, які є компонентами безпеки в розумінні Регламенту (ЄС) 2024/1689 Європейського Парламенту та Ради (*), враховуються вимоги, встановлені в главі III, розділі 2, цього Регламенту.

(*) Регламент (ЄС) 2024/1689 Європейського Парламенту та Ради від 13 червня 2024 року, що встановлює гармонізовані правила щодо штучного інтелекту та вносить зміни до Регламентів (ЄС) № 300/2008, (ЄС) № 167/2013, (ЄС) № 168/2013, (ЄС) 2018/858, (ЄС) 2018/1139 та (ЄС) 2019/2144 і Директив 2014/90/ЄС, (ЄС) 2016/797 та (ЄС) 2020/1828 (Акт про штучний інтелект) (OJ L, 2024/1689, 12.7.2024, ELI: http://data.europa.eu/eli/reg/2024/1689/oj).';"

(2) до статті 19 додається такий пункт:

'4. При ухваленні делегованих актів відповідно до пунктів 1 та 2, що стосуються систем штучного інтелекту, які є компонентами безпеки в розумінні Регламенту (ЄС) 2024/1689, враховуються вимоги, встановлені в главі III, розділі 2, цього Регламенту.'

;

(3) до статті 43 додається такий пункт:

'4. При ухваленні імплементаційних актів відповідно до пункту 1, що стосуються систем штучного інтелекту, які є компонентами безпеки

	в розумінні Регламенту (ЄС) 2024/1689, враховуються вимоги, встановлені в главі III, розділі 2, цього Регламенту.'
	;
(4)	до статті 47 додається такий пункт:
	'3. При ухваленні делегованих актів відповідно до пунктів 1 та 2, що стосуються систем штучного інтелекту, які є компонентами безпеки в розумінні Регламенту (ЄС) 2024/1689, враховуються вимоги, встановлені в главі III, розділі 2, цього Регламенту.'
	;
(5)	до статті 57 додається такий підпункт:
	'При ухваленні цих імплементаційних актів, що стосуються систем штучного інтелекту, які є компонентами безпеки в розумінні Регламенту (ЄС) 2024/1689, враховуються вимоги, встановлені в главі III, розділі 2, цього Регламенту.'
	;
(6)	до статті 58 додається такий пункт:
	'3. При ухваленні делегованих актів відповідно до пунктів 1 та 2, що стосуються систем штучного інтелекту, які є компонентами безпеки в розумінні Регламенту (ЄС) 2024/1689, враховуються вимоги, встановлені в главі III, розділі 2, цього Регламенту.'.

Стаття 109

Внесення змін до Регламенту (ЄС) 2019/2144

До статті 11 Регламенту (ЄС) 2019/2144 додається такий пункт:

'3. При ухваленні імплементаційних актів відповідно до пункту 2, що стосуються систем штучного інтелекту, які є компонентами безпеки в розумінні Регламенту (ЄС) 2024/1689 Європейського Парламенту та Ради (*), враховуються вимоги, встановлені в главі III, розділі 2, цього Регламенту.

Стаття 110

Внесення змін до Директиви (ЄС) 2020/1828

До Додатку I до Директиви (ЄС) 2020/1828 Європейського Парламенту та Ради (58), додається такий пункт:

'(68)	Регламент (ЄС) 2024/1689 Європейського Парламенту та Ради від 13 червня 2024 року, що встановлює гармонізовані правила щодо штучного інтелекту та вносить зміни до Регламентів (ЄС) № 300/2008, (ЄС) № 167/2013, (ЄС) № 168/2013, (ЄС) 2018/858, (ЄС) 2018/1139 та (ЄС) 2019/2144 і Директив 2014/90/ЄС, (ЄС) 2016/797 та (ЄС) 2020/1828 (Акт про штучний інтелект) (OJ L, 2024/1689, 12.7.2024, ELI: http://data.europa.eu/eli/reg/2024/1689/oj).'.

Стаття 111

Системи штучного інтелекту, вже введені в обіг або введені в експлуатацію, та моделі штучного інтелекту загального призначення, вже введені в обіг

1. Без шкоди для застосування статті 5, як зазначено в статті 113(3), пункті (a), системи штучного інтелекту, що є компонентами великомасштабних ІТ-систем, створених правовими актами, переліченими в Додатку X, які були введені в обіг або введені в експлуатацію до 2 серпня 2027 року, приводяться у відповідність із цим Регламентом до 31 грудня 2030 року.

Вимоги, встановлені в цьому Регламенті, беруться до уваги при оцінці кожної великомасштабної ІТ-системи, створеної правовими актами, переліченими в Додатку X, яка має проводитися відповідно до цих правових актів, та у випадку заміни або внесення змін до цих правових актів.

2. Без шкоди для застосування статті 5, як зазначено в статті 113(3), пункті (a), цей Регламент застосовується до операторів високоризикових систем штучного інтелекту, окрім систем, зазначених у пункті 1 цієї статті, що були введені в обіг або введені в експлуатацію до 2 серпня 2026 року, лише якщо з цієї дати ці системи зазнали суттєвих змін у своїх конструкціях. У будь-якому разі постачальники та суб'єкти розгортання високоризикових систем штучного інтелекту, призначених для використання органами публічної влади, вживають необхідних заходів для дотримання вимог та зобов'язань цього Регламенту до 2 серпня 2030 року.

3. Постачальники моделей штучного інтелекту загального призначення, які були введені в обіг до 2 серпня 2025 року, вживають необхідних заходів для дотримання зобов'язань, встановлених у цьому Регламенті, до 2 серпня 2027 року.

Стаття 112

Оцінка та перегляд

1. Комісія оцінює необхідність внесення змін до переліку, встановленого в Додатку III, та до переліку заборонених практик штучного інтелекту, встановлених у статті 5, один раз на рік після набрання чинності цим Регламентом та до закінчення строку делегування повноважень, встановленого в статті 97. Комісія подає висновки цієї оцінки Європейському Парламенту та Раді.

2. До 2 серпня 2028 року та кожні чотири роки після цього Комісія оцінює та звітує Європейському Парламенту та Раді щодо такого:

(а) необхідності внесення змін, що розширюють існуючі заголовки областей або додають нові заголовки областей у Додатку III;

(б) змін до переліку систем штучного інтелекту, що вимагають додаткових заходів щодо прозорості, у статті 50;

(в) змін, що підвищують ефективність системи нагляду та управління.

3. До 2 серпня 2029 року та кожні чотири роки після цього Комісія подає звіт про оцінку та перегляд цього Регламенту Європейському Парламенту та Раді. Звіт включає оцінку структури виконання та можливої необхідності агентства Союзу для усунення будь-яких виявлених недоліків. На підставі висновків цей звіт у відповідних випадках супроводжується пропозицією щодо внесення змін до цього Регламенту. Звіти оприлюднюються.

4. Звіти, зазначені в пункті 2, приділяють особливу увагу такому:

(а) стан фінансових, технічних та людських ресурсів національних компетентних органів для ефективного виконання завдань, покладених на них відповідно до цього Регламенту;

(б) стан санкцій, зокрема адміністративних штрафів, зазначених у статті 99(1), що застосовуються державами-членами за порушення цього Регламенту;

(в) ухвалені гармонізовані стандарти та спільні специфікації, розроблені на підтримку цього Регламенту;

(г) кількість підприємств, що виходять на ринок після набрання чинності цим Регламентом, та скільки з них є МСП.

5. До 2 серпня 2028 року Комісія оцінює функціонування Офісу зі штучного інтелекту, чи були надані Офісу зі штучного інтелекту достатні повноваження та компетенції для виконання своїх завдань, та чи є доцільним і необхідним для належного виконання та застосування цього Регламенту підвищення рівня Офісу зі штучного інтелекту, його повноважень у сфері виконання та збільшення його ресурсів. Комісія подає звіт про свою оцінку Європейському Парламенту та Раді.

6. До 2 серпня 2028 року та кожні чотири роки після цього Комісія подає звіт про перегляд прогресу щодо розробки стандартизаційних результатів з енергоефективної розробки моделей штучного інтелекту загального призначення та оцінює необхідність подальших заходів або дій, включаючи обов'язкові заходи або дії. Звіт подається Європейському Парламенту та Раді та оприлюднюється.

7. До 2 серпня 2028 року та кожні три роки після цього Комісія оцінює вплив та ефективність добровільних кодексів поведінки для сприяння застосуванню вимог, встановлених у главі III, розділі 2, для систем штучного інтелекту, окрім високоризикових систем штучного інтелекту, та можливих

інших додаткових вимог до систем штучного інтелекту, окрім високоризикових систем штучного інтелекту, у тому числі щодо екологічної стійкості.

8. Для цілей пунктів 1–7 Рада, держави-члени та національні компетентні органи надають Комісії інформацію на її запит та без зайвих зволікань.

9. Проводячи оцінки та перегляди, зазначені в пунктах 1–7, Комісія враховує позиції та висновки Ради, Європейського Парламенту, Ради міністрів та інших відповідних органів або джерел.

10. Комісія за необхідності подає відповідні пропозиції щодо внесення змін до цього Регламенту, зокрема з урахуванням розвитку технологій, впливу систем штучного інтелекту на здоров'я та безпеку та на основоположні права, а також з огляду на стан прогресу в інформаційному суспільстві.

11. Для керівництва оцінками та переглядами, зазначеними в пунктах 1–7 цієї статті, Офіс зі штучного інтелекту зобов'язується розробити об'єктивну та партисипативну методологію оцінки рівнів ризику на основі критеріїв, визначених у відповідних статтях, та включення нових систем до:

(а) переліку, встановленого в Додатку III, включаючи розширення існуючих заголовків областей або додавання нових заголовків областей до цього Додатку;

(б) переліку заборонених практик, встановлених у статті 5; та

(в) переліку систем штучного інтелекту, що вимагають додаткових заходів щодо прозорості відповідно до статті 50.

12. Будь-які зміни до цього Регламенту відповідно до пункту 10, або відповідні делеговані чи імплементаційні акти, що стосуються галузевого законодавства Союзу про гармонізацію, переліченого в розділі B Додатку I, враховують регуляторну специфіку кожного сектору та існуючі механізми та органи управління, оцінки відповідності та виконання, встановлені в ньому.

13. До 2 серпня 2031 року Комісія проводить оцінку виконання цього Регламенту та звітує про неї Європейському Парламенту, Раді та Європейському економічному та соціальному комітету з урахуванням перших років застосування цього Регламенту. На підставі висновків цей звіт у відповідних випадках супроводжується пропозицією щодо внесення змін до цього Регламенту стосовно структури виконання та необхідності агентства Союзу для усунення будь-яких виявлених недоліків.

Стаття 113

Набрання чинності та застосування

Цей Регламент набирає чинності на двадцятий день після його публікації в Офіційному журналі Європейського Союзу.

Він застосовується з 2 серпня 2026 року.

Однак:

(а) Глави I та II застосовуються з 2 лютого 2025 року;

(б)	Глава III, розділ 4, Глава V, Глава VII та Глава XII, а також стаття 78 застосовуються з 2 серпня 2025 року, за винятком статті 101;
(в)	Стаття 6(1) та відповідні зобов'язання в цьому Регламенті застосовуються з 2 серпня 2027 року.

Цей Регламент є обов'язковим у повному обсязі та безпосередньо застосовним у всіх державах-членах.

Вчинено в Брюсселі, 13 червня 2024 року.

За Європейський Парламент

Президент

Р. МЕЦОЛА

За Раду

Президент

М. МІШЕЛЬ

---

(1)OJ C 517, 22.12.2021, p. 56.

(2)OJ C 115, 11.3.2022, p. 5.

(3)OJ C 97, 28.2.2022, p. 60.

(4) Позиція Європейського Парламенту від 13 березня 2024 року (ще не опублікована в Офіційному віснику) та рішення Ради від 21 травня 2024 року.

(5) Рада Євросоюзу, Спеціальне засідання Європейської Ради (1 і 2 жовтня 2020 року) — Висновки, EUCO 13/20, 2020, с. 6.

(6) Резолюція Європейського Парламенту від 20 жовтня 2020 року з рекомендаціями Комісії щодо засад етичних аспектів штучного інтелекту, робототехніки та пов'язаних технологій, 2020/2012(INL).

(7) Регламент (ЄС) № 765/2008 Європейського Парламенту та Ради від 9 липня 2008 року, що встановлює вимоги до акредитації та скасовує Регламент (ЄЕС) № 339/93 (OJ L 218, 13.8.2008, p. 30).

(8) Рішення № 768/2008/ЄС Європейського Парламенту та Ради від 9 липня 2008 року про спільну базу для реалізації продуктів на ринку та скасування Рішення Ради 93/465/ЄЕС (OJ L 218, 13.8.2008, p. 82).

(9) Регламент (ЄС) 2019/1020 Європейського Парламенту та Ради від 20 червня 2019 року про ринковий нагляд та відповідність продуктів та внесення змін до Директиви 2004/42/ЄС та Регламентів (ЄС) № 765/2008 та (ЄС) № 305/2011 (OJ L 169, 25.6.2019, p. 1).

(10) Директива Ради 85/374/ЄЕС від 25 липня 1985 року про зближення законів, нормативних актів та адміністративних положень держав-членів щодо відповідальності за дефектні продукти (OJ L 210, 7.8.1985, p. 29).

(11) Регламент (ЄС) 2016/679 Європейського Парламенту та Ради від 27 квітня 2016 року про захист фізичних осіб стосовно обробки персональних даних та про вільний рух таких даних, і скасування Директиви 95/46/ЄС (Загальний регламент про захист даних) (OJ L 119, 4.5.2016, p. 1).

(12) Регламент (ЄС) 2018/1725 Європейського Парламенту та Ради від 23 жовтня 2018 року про захист фізичних осіб стосовно обробки персональних даних інституціями, органами, офісами та агентствами Союзу та про вільний рух таких даних і скасування Регламенту (ЄС) № 45/2001 та Рішення № 1247/2002/ЄС (OJ L 295, 21.11.2018, p. 39).

(13) Директива (ЄС) 2016/680 Європейського Парламенту та Ради від 27 квітня 2016 року про захист фізичних осіб стосовно обробки персональних даних компетентними органами з метою попередження, розслідування, виявлення чи переслідування кримінальних злочинів або виконання кримінальних покарань, та про вільний рух таких даних, та скасування Рамкового рішення Ради 2008/977/ПВД (OJ L 119, 4.5.2016, p. 89).

(14) Директива 2002/58/ЄС Європейського Парламенту та Ради від 12 липня 2002 року стосовно обробки персональних даних та захисту конфіденційності в секторі електронних комунікацій (Директива про конфіденційність та електронні комунікації) (OJ L 201, 31.7.2002, p. 37).

(15) Регламент (ЄС) 2022/2065 Європейського Парламенту та Ради від 19 жовтня 2022 року про єдиний ринок цифрових послуг та внесення змін до Директиви 2000/31/ЄС (Акт про цифрові послуги) (OJ L 277, 27.10.2022, p. 1).

(16) Директива (ЄС) 2019/882 Європейського Парламенту та Ради від 17 квітня 2019 року про вимоги доступності для продуктів та послуг (OJ L 151, 7.6.2019, p. 70).

(17) Директива 2005/29/ЄС Європейського Парламенту та Ради від 11 травня 2005 року щодо недобросовісних комерційних практик між підприємствами та споживачами на внутрішньому ринку та внесення змін до Директиви Ради 84/450/ЄЕС, Директив 97/7/ЄС, 98/27/ЄС та 2002/65/ЄС Європейського Парламенту та Ради та Регламенту (ЄС) № 2006/2004 Європейського Парламенту та Ради (Директива про недобросовісні комерційні практики) (OJ L 149, 11.6.2005, p. 22).

(18) Рамкове рішення Ради 2002/584/ПВД від 13 червня 2002 року про Європейський ордер на арешт та процедури передачі між державами-членами (OJ L 190, 18.7.2002, p. 1).

(19) Директива (ЄС) 2022/2557 Європейського Парламенту та Ради від 14 грудня 2022 року про стійкість критичних суб'єктів та скасування Директиви Ради 2008/114/ЄС (OJ L 333, 27.12.2022, p. 164).

(20)OJ C 247, 29.6.2022, p. 1.

(21) Регламент (ЄС) 2017/745 Європейського Парламенту та Ради від 5 квітня 2017 року про медичні вироби, внесення змін до Директиви 2001/83/ЄС, Регламентів (ЄС) № 178/2002 та (ЄС) № 1223/2009 та скасування Директив Ради 90/385/ЄЕС та 93/42/ЄЕС (OJ L 117, 5.5.2017, p. 1).

(22) Регламент (ЄС) 2017/746 Європейського Парламенту та Ради від 5 квітня 2017 року про in vitro діагностичні медичні вироби in vitro та скасування Директиви 98/79/ЄС та Рішення Комісії 2010/227/ЄС (OJ L 117, 5.5.2017, p. 176).

(23) Директива 2006/42/ЄС Європейського Парламенту та Ради від 17 травня 2006 року про машини та внесення змін до Директиви 95/16/ЄС (OJ L 157, 9.6.2006, p. 24).

(24) Регламент (ЄС) № 300/2008 Європейського Парламенту та Ради від 11 березня 2008 року про загальні правила в галузі авіаційної безпеки та скасування Регламенту (ЄС) № 2320/2002 (OJ L 97, 9.4.2008, p. 72).

(25) Регламент (ЄС) № 167/2013 Європейського Парламенту та Ради від 5 лютого 2013 року про затвердження та ринковий нагляд сільськогосподарських та лісогосподарських транспортних засобів (OJ L 60, 2.3.2013, p. 1).

(26) Регламент (ЄС) № 168/2013 Європейського Парламенту та Ради від 15 січня 2013 року про затвердження та ринковий нагляд двоколісних або триколісних транспортних засобів та квадрициклів (OJ L 60, 2.3.2013, p. 52).

(27) Директива 2014/90/ЄС Європейського Парламенту та Ради від 23 липня 2014 року про морське обладнання та скасування Директиви Ради 96/98/ЄС (OJ L 257, 28.8.2014, p. 146).

(28) Директива (ЄС) 2016/797 Європейського Парламенту та Ради від 11 травня 2016 року про сумісність залізничної системи в межах Європейського Союзу (OJ L 138, 26.5.2016, p. 44).

(29) Регламент (ЄС) 2018/858 Європейського Парламенту та Ради від 30 травня 2018 року про затвердження та ринковий нагляд автотранспортних засобів та їхніх причепів, а також систем, компонентів та окремих технічних блоків, призначених для таких транспортних засобів, внесення змін до Регламентів (ЄС) № 715/2007 та (ЄС) № 595/2009 та скасування Директиви 2007/46/ЄС (OJ L 151, 14.6.2018, p. 1).

(30) Регламент (ЄС) 2018/1139 Європейського Парламенту та Ради від 4 липня 2018 року про загальні правила в галузі цивільної авіації та створення Агентства авіаційної безпеки Європейського Союзу, внесення змін до Регламентів (ЄС) № 2111/2005, (ЄС) № 1008/2008, (ЄС) № 996/2010, (ЄС) № 376/2014 та Директив 2014/30/ЄС та 2014/53/ЄС Європейського Парламенту та Ради, та скасування Регламентів (ЄС) № 552/2004 та (ЄС) № 216/2008 Європейського Парламенту та Ради та Регламенту Ради (ЄЕС) № 3922/91 (OJ L 212, 22.8.2018, p. 1).

(31) Регламент (ЄС) 2019/2144 Європейського Парламенту та Ради від 27 листопада 2019 року про вимоги до типового затвердження автотранспортних засобів та їхніх причепів, а також систем, компонентів та окремих технічних блоків, призначених для таких транспортних засобів, щодо їхньої загальної безпеки та захисту учасників транспортних засобів та вразливих учасників дорожнього руху, внесення змін до Регламенту (ЄС) 2018/858 Європейського Парламенту та Ради та скасування Регламентів (ЄС) № 78/2009, (ЄС) № 79/2009 та (ЄС) № 661/2009 Європейського Парламенту та Ради та Регламентів Комісії (ЄС) № 631/2009, (ЄС) № 406/2010, (ЄС) № 672/2010, (ЄС) № 1003/2010, (ЄС) № 1005/2010, (ЄС) № 1008/2010, (ЄС) № 1009/2010, (ЄС) № 19/2011, (ЄС) № 109/2011, (ЄС) № 458/2011, (ЄС) № 65/2012, (ЄС) № 130/2012, (ЄС) № 347/2012, (ЄС) № 351/2012, (ЄС) № 1230/2012 та (ЄС) 2015/166 (OJ L 325, 16.12.2019, p. 1).

(32) Регламент (ЄС) № 810/2009 Європейського Парламенту та Ради від 13 липня 2009 року про встановлення Кодексу Співтовариства про візи (Візовий кодекс) (OJ L 243, 15.9.2009, p. 1).

(33) Директива 2013/32/ЄС Європейського Парламенту та Ради від 26 червня 2013 року про загальні процедури надання та скасування міжнародного захисту (OJ L 180, 29.6.2013, p. 60).

(34) Регламент (ЄС) 2024/900 Європейського Парламенту та Ради від 13 березня 2024 року про прозорість та цільову спрямованість політичної реклами (OJ L, 2024/900, 20.3.2024, ELI: http://data.europa.eu/eli/reg/2024/900/oj).

(35) Директива 2014/31/ЄС Європейського Парламенту та Ради від 26 лютого 2014 року про гармонізацію законів держав-членів щодо надання на ринку неавтоматичних вагових приладів (OJ L 96, 29.3.2014, p. 107).

(36) Директива 2014/32/ЄС Європейського Парламенту та Ради від 26 лютого 2014 року про гармонізацію законів держав-членів щодо надання на ринку вимірювальних приладів (OJ L 96, 29.3.2014, p. 149).

(37) Регламент (ЄС) 2019/881 Європейського Парламенту та Ради від 17 квітня 2019 року про ENISA (Агентство Європейського Союзу з кібербезпеки) та про сертифікацію кібербезпеки інформаційних та комунікаційних технологій та скасування Регламенту (ЄС) № 526/2013 (Акт про кібербезпеку) (OJ L 151, 7.6.2019, p. 15).

(38) Директива (ЄС) 2016/2102 Європейського Парламенту та Ради від 26 жовтня 2016 року про доступність веб-сайтів та мобільних додатків органів публічного сектору (OJ L 327, 2.12.2016, p. 1).

(39) Директива 2002/14/ЄС Європейського Парламенту та Ради від 11 березня 2002 року про встановлення загальної бази для інформування та консультування працівників у Європейській Спільноті (OJ L 80, 23.3.2002, p. 29).

(40) Директива (ЄС) 2019/790 Європейського Парламенту та Ради від 17 квітня 2019 року про авторське право та суміжні права на Єдиному цифровому ринку та внесення змін до Директив 96/9/ЄС та 2001/29/ЄС (OJ L 130, 17.5.2019, p. 92).

(41) Регламент (ЄС) № 1025/2012 Європейського Парламенту та Ради від 25 жовтня 2012 року про Європейську стандартизацію, внесення змін до Директив Ради 89/686/ЄЕС та 93/15/ЄЕС та Директив 94/9/ЄС, 94/25/ЄС, 95/16/ЄС, 97/23/ЄС, 98/34/ЄС, 2004/22/ЄС, 2007/23/ЄС, 2009/23/ЄС та 2009/105/ЄС Європейського Парламенту та Ради та скасування Рішення Ради 87/95/ЄЕС та Рішення № 1673/2006/ЄС Європейського Парламенту та Ради (OJ L 316, 14.11.2012, p. 12).

(42) Регламент (ЄС) 2022/868 Європейського Парламенту та Ради від 30 травня 2022 року про Європейське управління даними та внесення змін до Регламенту (ЄС) 2018/1724 (Акт про управління даними) (OJ L 152, 3.6.2022, p. 1).

(43) Регламент (ЄС) 2023/2854 Європейського Парламенту та Ради від 13 грудня 2023 року про гармонізовані правила справедливого доступу до даних та їх використання та внесення змін до Регламенту (ЄС) 2017/2394 та Директиви (ЄС) 2020/1828 (Акт про дані) (OJ L, 2023/2854, 22.12.2023, ELI: http://data.europa.eu/eli/reg/2023/2854/oj).

(44) Рекомендація Комісії від 6 травня 2003 року щодо визначення мікро-, малих та середніх підприємств (OJ L 124, 20.5.2003, p. 36).

(45) Рішення Комісії від 24.1.2024 про заснування Європейського офісу зі штучного інтелекту C(2024) 390.

(46) Регламент (ЄС) № 575/2013 Європейського Парламенту та Ради від 26 червня 2013 року про пруденційні вимоги до кредитних установ та інвестиційних компаній та внесення змін до Регламенту (ЄС) № 648/2012 (OJ L 176, 27.6.2013, p. 1).

(47) Директива 2008/48/ЄС Європейського Парламенту та Ради від 23 квітня 2008 року про кредитні угоди для споживачів та скасування Директиви Ради 87/102/ЄЕС (OJ L 133, 22.5.2008, p. 66).

(48) Директива 2009/138/ЄС Європейського Парламенту та Ради від 25 листопада 2009 року про початок та здійснення діяльності зі страхування та перестрахування (Solvency II) (OJ L 335, 17.12.2009, p. 1).

(49) Директива 2013/36/ЄС Європейського Парламенту та Ради від 26 червня 2013 року про доступ до діяльності кредитних установ та пруденційний нагляд за кредитними установами та інвестиційними компаніями, внесення змін до Директиви 2002/87/ЄС та скасування Директив 2006/48/ЄС та 2006/49/ЄС (OJ L 176, 27.6.2013, p. 338).

(50) Директива 2014/17/ЄС Європейського Парламенту та Ради від 4 лютого 2014 року про кредитні угоди для споживачів стосовно житлової нерухомості та внесення змін до Директив 2008/48/ЄС та 2013/36/ЄС та Регламенту (ЄС) № 1093/2010 (OJ L 60, 28.2.2014, p. 34).

(51) Директива (ЄС) 2016/97 Європейського Парламенту та Ради від 20 січня 2016 року про розповсюдження страхування (OJ L 26, 2.2.2016, p. 19).

(52) Регламент Ради (ЄС) № 1024/2013 від 15 жовтня 2013 року про покладення на Європейський центральний банк конкретних завдань стосовно політик, пов'язаних з пруденційним наглядом за кредитними установами (OJ L 287, 29.10.2013, p. 63).

(53) Регламент (ЄС) 2023/988 Європейського Парламенту та Ради від 10 травня 2023 року про загальну безпечність продуктів, внесення змін до Регламенту (ЄС) № 1025/2012 Європейського Парламенту та Ради та Директиви (ЄС) 2020/1828 Європейського Парламенту та Ради, та скасування Директиви 2001/95/ЄС Європейського Парламенту та Ради та Директиви Ради 87/357/ЄЕС (OJ L 135, 23.5.2023, p. 1).

(54) Директива (ЄС) 2019/1937 Європейського Парламенту та Ради від 23 жовтня 2019 року про захист осіб, які повідомляють про порушення права Союзу (OJ L 305, 26.11.2019, p. 17).

(55)OJ L 123, 12.5.2016, p. 1.

(56) Регламент (ЄС) № 182/2011 Європейського Парламенту та Ради від 16 лютого 2011 року, що встановлює правила та загальні принципи щодо механізмів контролю державами-членами здійснення Комісією виконавчих повноважень (OJ L 55, 28.2.2011, p. 13).

(57) Директива (ЄС) 2016/943 Європейського Парламенту та Ради від 8 червня 2016 року про захист нерозкритого ноу-хау та комерційної інформації (торгових таємниць) від їх незаконного отримання, використання та розкриття (OJ L 157, 15.6.2016, p. 1).

(58) Директива (ЄС) 2020/1828 Європейського Парламенту та Ради від 25 листопада 2020 року про представницькі дії для захисту колективних інтересів споживачів та скасування Директиви 2009/22/ЄС (OJ L 409, 4.12.2020, p. 1).

ДОДАТОК I

Перелік законодавства Союзу про гармонізацію

Розділ А. Перелік законодавства Союзу про гармонізацію на основі Нової законодавчої бази

1.	Директива 2006/42/ЄС Європейського Парламенту та Ради від 17 травня 2006 року про машини та про внесення змін до Директиви 95/16/ЄС (OJ L 157, 9.6.2006, p. 24);
2.	Директива 2009/48/ЄС Європейського Парламенту та Ради від 18 червня 2009 року про безпечність іграшок (OJ L 170, 30.6.2009, p. 1);
3.	Директива 2013/53/ЄС Європейського Парламенту та Ради від 20 листопада 2013 року про рекреаційні судна та гідроцикли та про скасування Директиви 94/25/ЄС (OJ L 354, 28.12.2013, p. 90);
4.	Директива 2014/33/ЄС Європейського Парламенту та Ради від 26 лютого 2014 року про гармонізацію законодавства держав-членів щодо ліфтів та захисних компонентів для ліфтів (OJ L 96, 29.3.2014, p. 251);
5.	Директива 2014/34/ЄС Європейського Парламенту та Ради від 26 лютого 2014 року про гармонізацію законодавства держав-членів щодо обладнання та захисних систем, призначених для використання у потенційно вибухонебезпечних середовищах (OJ L 96, 29.3.2014, p. 309);
6.	Директива 2014/53/ЄС Європейського Парламенту та Ради від 16 квітня 2014 року про гармонізацію законодавства

держав-членів щодо надання в розпорядження на ринку радіообладнання та про скасування Директиви 1999/5/ЄС (OJ L 153, 22.5.2014, p. 62);

7. Директива 2014/68/ЄС Європейського Парламенту та Ради від 15 травня 2014 року про гармонізацію законодавства держав-членів щодо надання в розпорядження на ринку обладнання, що працює під тиском (OJ L 189, 27.6.2014, p. 164);

8. Регламент (ЄС) 2016/424 Європейського Парламенту та Ради від 9 березня 2016 року про канатні дороги та про скасування Директиви 2000/9/ЄС (OJ L 81, 31.3.2016, p. 1);

9. Регламент (ЄС) 2016/425 Європейського Парламенту та Ради від 9 березня 2016 року про засоби індивідуального захисту та про скасування Директиви Ради 89/686/ЄЕС (OJ L 81, 31.3.2016, p. 51);

10. Регламент (ЄС) 2016/426 Європейського Парламенту та Ради від 9 березня 2016 року про прилади, що спалюють газоподібне паливо, та про скасування Директиви 2009/142/ЄС (OJ L 81, 31.3.2016, p. 99);

11. Регламент (ЄС) 2017/745 Європейського Парламенту та Ради від 5 квітня 2017 року про медичні вироби, про внесення змін до Директиви 2001/83/ЄС, Регламенту (ЄС) № 178/2002 та Регламенту (ЄС) № 1223/2009 та про скасування Директив Ради 90/385/ЄЕС та 93/42/ЄЕС (OJ L 117, 5.5.2017, p. 1);

12.	Регламент (ЄС) 2017/746 Європейського Парламенту та Ради від 5 квітня 2017 року про in vitro діагностичні медичні вироби in vitro та про скасування Директиви 98/79/ЄС та Рішення Комісії 2010/227/ЄС (OJ L 117, 5.5.2017, p. 176).

Розділ B. Перелік іншого законодавства Союзу про гармонізацію

13.	Регламент (ЄС) № 300/2008 Європейського Парламенту та Ради від 11 березня 2008 року про загальні правила у сфері авіаційної безпеки та про скасування Регламенту (ЄС) № 2320/2002 (OJ L 97, 9.4.2008, p. 72);
14.	Регламент (ЄС) № 168/2013 Європейського Парламенту та Ради від 15 січня 2013 року про затвердження та ринковий нагляд за дво- або триколісними транспортними засобами та квадроциклами (OJ L 60, 2.3.2013, p. 52);
15.	Регламент (ЄС) № 167/2013 Європейського Парламенту та Ради від 5 лютого 2013 року про затвердження та ринковий нагляд за сільськогосподарськими та лісовими транспортними засобами (OJ L 60, 2.3.2013, p. 1);
16.	Директива 2014/90/ЄС Європейського Парламенту та Ради від 23 липня 2014 року про морське обладнання та про скасування Директиви Ради 96/98/ЄС (OJ L 257, 28.8.2014, p. 146);
17.	Директива (ЄС) 2016/797 Європейського Парламенту та Ради від 11 травня 2016 року про сумісність залізничної системи в

межах Європейського Союзу (OJ L 138, 26.5.2016, p. 44);

18. Регламент (ЄС) 2018/858 Європейського Парламенту та Ради від 30 травня 2018 року про затвердження та ринковий нагляд за моторними транспортними засобами та їхніми причепами, а також системами, компонентами та окремими технічними вузлами, призначеними для таких транспортних засобів, про внесення змін до Регламентів (ЄС) № 715/2007 та (ЄС) № 595/2009 та про скасування Директиви 2007/46/ЄС (OJ L 151, 14.6.2018, p. 1);

19. Регламент (ЄС) 2019/2144 Європейського Парламенту та Ради від 27 листопада 2019 року про вимоги до затвердження типу моторних транспортних засобів та їхніх причепів, а також систем, компонентів та окремих технічних вузлів, призначених для таких транспортних засобів, щодо їхньої загальної безпеки та захисту водіїв і вразливих учасників дорожнього руху, про внесення змін до Регламенту (ЄС) 2018/858 Європейського Парламенту та Ради та про скасування Регламентів (ЄС) № 78/2009, (ЄС) № 79/2009 та (ЄС) № 661/2009 Європейського Парламенту та Ради та Регламентів Комісії (ЄС) № 631/2009, (ЄС) № 406/2010, (ЄС) № 672/2010, (ЄС) № 1003/2010, (ЄС) № 1005/2010, (ЄС) № 1008/2010, (ЄС) № 1009/2010, (ЄС) № 19/2011, (ЄС) № 109/2011, (ЄС) № 458/2011, (ЄС) № 65/2012, (ЄС) № 130/2012, (ЄС) № 347/2012, (ЄС)

	№ 351/2012, (ЄС) № 1230/2012 та (ЄС) 2015/166 (OJ L 325, 16.12.2019, p. 1);
20.	Регламент (ЄС) 2018/1139 Європейського Парламенту та Ради від 4 липня 2018 року про загальні правила у сфері цивільної авіації та про заснування Агентства авіаційної безпеки Європейського Союзу, про внесення змін до Регламентів (ЄС) № 2111/2005, (ЄС) № 1008/2008, (ЄС) № 996/2010, (ЄС) № 376/2014 та Директив 2014/30/ЄС та 2014/53/ЄС Європейського Парламенту та Ради та про скасування Регламентів (ЄС) № 552/2004 та (ЄС) № 216/2008 Європейського Парламенту та Ради та Регламенту Ради (ЄЕС) № 3922/91 (OJ L 212, 22.8.2018, p. 1), у частині, що стосується проектування, виробництва та введення в обіг повітряних суден, зазначених у статті 2(1), пунктах (а) та (б) цього регламенту, у тій мірі, в якій це стосується безпілотних повітряних суден та їхніх двигунів, гвинтів, частин та обладнання для дистанційного керування ними.

ДОДАТОК II

Перелік кримінальних правопорушень, зазначених у статті 5(1), першому підпункті, пункті (h)(iii)

Кримінальні правопорушення, зазначені в статті 5(1), першому підпункті, пункті (h)(iii):

— тероризм,

— торгівля людьми,

— сексуальна експлуатація дітей та дитяча порнографія,

— незаконний обіг наркотичних або психотропних речовин,

— незаконна торгівля зброєю, боєприпасами або вибуховими речовинами,

— вбивство, тяжке тілесне ушкодження,

— незаконна торгівля людськими органами або тканинами,

— незаконний обіг ядерних або радіоактивних матеріалів,

— викрадення людини, незаконне позбавлення волі або захоплення заручників,

— злочини, що підпадають під юрисдикцію Міжнародного кримінального суду,

— незаконне захоплення повітряних суден або суден,

— зґвалтування,

— злочини проти довкілля,

— організований або збройний грабіж,

— саботаж,

— участь у злочинній організації, причетній до одного або кількох правопорушень, перелічених вище.

ДОДАТОК III

Високоризикові системи штучного інтелекту, зазначені в статті 6(2)

Високоризиковими системами штучного інтелекту відповідно до статті 6(2) є системи штучного інтелекту, перелічені в будь-якій із таких сфер:

1. Біометрія, тією мірою, якою їх використання дозволено відповідним законодавством Союзу або національним законодавством:

   (а) системи дистанційної біометричної ідентифікації.

   Сюди не входять системи штучного інтелекту, призначені для використання з метою біометричної верифікації, єдиною метою якої є підтвердження того, що конкретна фізична особа є тією особою, за яку вона себе видає;

   (б) системи штучного інтелекту, призначені для використання з метою біометричної категоризації відповідно до чутливих або захищених атрибутів чи характеристик на основі висновку про ці атрибути або характеристики;

   (в) системи штучного інтелекту, призначені для використання з метою розпізнавання емоцій.

2. Критична інфраструктура: системи штучного інтелекту, призначені для використання як компоненти безпеки в управлінні та

функціонуванні критичної цифрової інфраструктури, дорожнього руху або у постачанні води, газу, тепла або електроенергії.

3. Освіта та професійна підготовка:

(а) системи штучного інтелекту, призначені для використання з метою визначення доступу або зарахування чи призначення фізичних осіб до освітніх та навчальних закладів усіх рівнів;

(б) системи штучного інтелекту, призначені для використання з метою оцінки результатів навчання, у тому числі коли ці результати використовуються для скерування процесу навчання фізичних осіб в освітніх та навчальних закладах усіх рівнів;

(в) системи штучного інтелекту, призначені для використання з метою оцінки відповідного рівня освіти, який особа отримає або матиме змогу отримати, в контексті або в межах освітніх та навчальних закладів усіх рівнів;

(г) системи штучного інтелекту, призначені для використання з метою моніторингу та виявлення забороненої поведінки студентів під

час тестів у контексті або в межах освітніх та навчальних закладів усіх рівнів.

4. Зайнятість, управління працівниками та доступ до самозайнятості:

(а) системи штучного інтелекту, призначені для використання з метою набору або відбору фізичних осіб, зокрема для розміщення цільових оголошень про роботу, аналізу та фільтрації заявок про прийняття на роботу та оцінки кандидатів;

(б) системи штучного інтелекту, призначені для використання з метою прийняття рішень, що впливають на умови трудових відносин, підвищення або припинення трудових договірних відносин, розподілу завдань на основі індивідуальної поведінки чи особистих рис або характеристик або моніторингу та оцінки результатів і поведінки осіб у таких відносинах.

5. Доступ до основних приватних послуг та основних публічних послуг і виплат та користування ними:

(а) системи штучного інтелекту, призначені для використання державними органами або від імені

державних органів для оцінки права фізичних осіб на основні виплати та послуги публічної допомоги, включаючи послуги охорони здоров'я, а також для надання, зменшення, відкликання або повернення таких виплат і послуг;

(б) системи штучного інтелекту, призначені для використання з метою оцінки кредитоспроможності фізичних осіб або встановлення їхнього кредитного рейтингу, за винятком систем штучного інтелекту, що використовуються для виявлення фінансового шахрайства;

(в) системи штучного інтелекту, призначені для використання з метою оцінки ризиків та встановлення цін стосовно фізичних осіб у разі страхування життя та здоров'я;

(г) системи штучного інтелекту, призначені для оцінки та класифікації екстрених викликів фізичних осіб або для використання з метою диспетчеризації або встановлення пріоритетів при диспетчеризації служб першого екстреного реагування, у тому числі поліції, пожежників та

медичної допомоги, а також систем тріажу пацієнтів екстреної медичної допомоги.

6. Правоохоронна діяльність, тією мірою, якою їх використання дозволено відповідним законодавством Союзу або національним законодавством:

(а) системи штучного інтелекту, призначені для використання правоохоронними органами або від їхнього імені, або інституціями, органами, службами чи агентствами Союзу на підтримку правоохоронних органів або від їхнього імені для оцінки ризику того, що фізична особа стане жертвою кримінальних правопорушень;

(б) системи штучного інтелекту, призначені для використання правоохоронними органами або від їхнього імені або інституціями, органами, службами чи агентствами Союзу на підтримку правоохоронних органів як поліграфи або аналогічні інструменти;

(в) системи штучного інтелекту, призначені для використання правоохоронними органами або від їхнього імені, або

інституціями, органами, службами чи агентствами Союзу на підтримку правоохоронних органів для оцінки достовірності доказів у ході розслідування або судового переслідування за кримінальні правопорушення;

(г) системи штучного інтелекту, призначені для використання правоохоронними органами або від їхнього імені або інституціями, органами, службами чи агентствами Союзу на підтримку правоохоронних органів для оцінки ризику вчинення або повторного вчинення правопорушення фізичною особою не виключно на основі профілювання фізичних осіб, як зазначено в статті 3(4) Директиви (ЄС) 2016/680, або для оцінки особистісних рис і характеристик або минулої злочинної поведінки фізичних осіб або груп;

(д) системи штучного інтелекту, призначені для використання правоохоронними органами або від їхнього імені або інституціями,

органами, службами чи агентствами Союзу на підтримку правоохоронних органів для профілювання фізичних осіб, як зазначено в статті 3(4) Директиви (ЄС) 2016/680, у ході виявлення, розслідування або судового переслідування за кримінальні правопорушення.

7. Міграція, притулок та управління прикордонним контролем, тією мірою, якою їх використання дозволено відповідним законодавством Союзу або національним законодавством:

(а) системи штучного інтелекту, призначені для використання компетентними державними органами або від їхнього імені або інституціями, органами, службами чи агентствами Союзу як поліграфи або аналогічні інструменти;

(б) системи штучного інтелекту, призначені для використання компетентними державними органами або від їхнього імені або інституціями, органами, службами чи агентствами Союзу для оцінки ризику, включаючи ризик безпеки, ризик нерегулярної міграції або ризик для здоров'я,

що його становить фізична особа, яка має намір в'їхати або в'їхала на територію держави-члена;

(в) системи штучного інтелекту, призначені для використання компетентними державними органами або від їхнього імені або інституціями, органами, службами чи агентствами Союзу для допомоги компетентним державним органам у розгляді заяв про надання притулку, візи або дозволів на проживання та пов'язаних скарг щодо права фізичних осіб, які подають заяву про отримання статусу, на такий статус, включаючи пов'язані оцінки достовірності доказів;

(г) системи штучного інтелекту, призначені для використання компетентними державними органами або від їхнього імені або інституціями, органами, службами чи агентствами Союзу в контексті управління міграцією, притулком або прикордонним контролем з метою виявлення, розпізнавання або ідентифікації фізичних

		осіб, за винятком перевірки проїзних документів.
8.	Відправлення правосуддя та демократичні процеси:	
	(а)	системи штучного інтелекту, призначені для використання судовим органом або від його імені для допомоги судовому органу в дослідженні та тлумаченні фактів і права та у застосуванні права до конкретної сукупності фактів або для використання аналогічним чином у альтернативному вирішенні спорів;
	(б)	системи штучного інтелекту, призначені для використання з метою впливу на результат виборів або референдуму або на поведінку фізичних осіб при голосуванні під час виборів або референдумів. Сюди не входять системи штучного інтелекту, результатам яких фізичні особи не піддаються безпосередньо, наприклад інструменти, що використовуються для організації, оптимізації або структурування виборчих кампаній з адміністративної або логістичної точки зору.

ДОДАТОК IV

Технічна документація, зазначена в статті 11(1)

Технічна документація, зазначена в статті 11(1), містить щонайменше таку інформацію, застосовну до відповідної системи штучного інтелекту:

1. Загальний опис системи штучного інтелекту, включаючи:

   (а) її призначення, найменування постачальника та версію системи, що відображає її зв'язок з попередніми версіями;

   (б) яким чином система штучного інтелекту взаємодіє або може використовуватися для взаємодії з апаратним або програмним забезпеченням, включаючи інші системи штучного інтелекту, що не є частиною самої системи штучного інтелекту, де це застосовно;

   (в) версії відповідного програмного або мікропрограмного забезпечення та будь-які вимоги, пов'язані з оновленнями версій;

   (г) опис усіх форм, у яких система штучного інтелекту виводиться на ринок або вводиться в експлуатацію, наприклад, програмні пакети, вбудовані в апаратне забезпечення, завантаження або API;

(д) опис апаратного забезпечення, на якому передбачається запускати систему штучного інтелекту;

(е) якщо система штучного інтелекту є компонентом продуктів, фотографії або ілюстрації, що відображають зовнішні характеристики, маркування та внутрішнє компонування цих продуктів;

(є) базовий опис інтерфейсу користувача, наданого суб'єкту розгортання;

(ж) інструкції з використання для суб'єкта розгортання та базовий опис інтерфейсу користувача, наданого суб'єкту розгортання, де це застосовно;

2. Детальний опис елементів системи штучного інтелекту та процесу її розроблення, включаючи:

(а) методи та кроки, виконані для розроблення системи штучного інтелекту, включаючи, де це доречно, звернення до попередньо навчених систем або інструментів, наданих третіми сторонами, та те, яким чином вони були використані,

інтегровані або модифіковані постачальником;

(б) технічні вимоги до системи, а саме загальна логіка системи штучного інтелекту та алгоритмів; ключові проєктні рішення, включаючи обґрунтування та зроблені припущення, у тому числі щодо осіб або груп осіб, для яких призначено систему; основні варіанти класифікації; для оптимізації чого призначено систему та значущість різних параметрів; опис очікуваних вихідних даних та якості вихідних даних системи; рішення щодо будь-яких можливих компромісів, прийнятих щодо технічних рішень, прийнятих для виконання вимог, встановлених у главі III, розділі 2;

(в) опис архітектури системи, що пояснює, яким чином програмні компоненти будуються один на одному або взаємодіють між собою та інтегруються в загальну обробку; обчислювальні ресурси, використані для розроблення,

навчання, тестування та валідації системи штучного інтелекту;

(г) де це доречно, вимоги до даних у вигляді паспортів даних, що описують методології та методи навчання та використані набори навчальних даних, включаючи загальний опис цих наборів даних, інформацію про їхнє походження, обсяг та основні характеристики; яким чином дані були отримані та відібрані; процедури маркування (наприклад, для навчання з учителем), методології очищення даних (наприклад, виявлення аномалій);

(д) оцінка заходів нагляду з боку людини, необхідних відповідно до статті 14, включаючи оцінку технічних заходів, необхідних для сприяння інтерпретації вихідних даних систем штучного інтелекту суб'єктами розгортання, відповідно до статті 13(3), пункту (d);

(е) де це застосовно, детальний опис заздалегідь визначених змін у системі штучного інтелекту та її роботі разом з усією відповідною інформацією,

пов'язаною з технічними рішеннями, прийнятими для забезпечення постійної відповідності системи штучного інтелекту відповідним вимогам, встановленим у главі III, розділі 2;

(є) використані процедури валідації та тестування, включаючи інформацію про використані дані валідації та тестування та їхні основні характеристики; метрики, використовувані для вимірювання точності, надійності та відповідності іншим відповідним вимогам, встановленим у главі III, розділі 2, а також потенційно дискримінаційні наслідки; журнали тестування та всі звіти про тестування, датовані та підписані відповідальними особами, у тому числі щодо заздалегідь визначених змін, зазначених у пункті (f);

(ж) вжиті заходи кібербезпеки;

3. Детальна інформація про моніторинг, функціонування та контроль системи штучного інтелекту, зокрема щодо: її можливостей та обмежень у роботі, включаючи ступені точності для конкретних осіб або груп осіб, для яких призначено систему, та загальний очікуваний

	рівень точності стосовно її призначення; передбачуваних ненавмисних результатів та джерел ризиків для здоров'я та безпеки, основних прав та дискримінації з огляду на призначення системи штучного інтелекту; заходів нагляду з боку людини, необхідних відповідно до статті 14, включаючи технічні заходи, вжиті для сприяння інтерпретації вихідних даних систем штучного інтелекту суб'єктами розгортання; специфікацій щодо вхідних даних, де це доречно;
4.	Опис доцільності метрик продуктивності для конкретної системи штучного інтелекту;
5.	Детальний опис системи управління ризиками відповідно до статті 9;
6.	Опис відповідних змін, внесених постачальником до системи протягом її життєвого циклу;
7.	Перелік гармонізованих стандартів, застосованих повністю або частково, посилання на які були опубліковані в Офіційному журналі Європейського Союзу; якщо такі гармонізовані стандарти не були застосовані, детальний опис рішень, прийнятих для виконання вимог, встановлених у главі III, розділі 2, включаючи перелік інших застосованих відповідних стандартів та технічних специфікацій;
8.	Копія декларації про відповідність ЄС, зазначена в статті 47;
9.	Детальний опис системи, що діє для оцінки продуктивності системи штучного інтелекту на постринковому етапі відповідно до статті 72, включаючи план постринкового моніторингу, зазначений у статті 72(3).

ДОДАТОК V

Декларація про відповідність ЄС

Декларація про відповідність ЄС, зазначена в статті 47, містить усю таку інформацію:

1.	Найменування та тип системи штучного інтелекту та будь-яке додаткове однозначне посилання, що дозволяє ідентифікацію та відстежуваність системи штучного інтелекту;
2.	Найменування та адреса постачальника або, де це застосовно, його уповноваженого представника;
3.	Заява про те, що декларація про відповідність ЄС, зазначена в статті 47, видається під виключну відповідальність постачальника;
4.	Заява про те, що система штучного інтелекту відповідає цьому Регламенту та, якщо це застосовно, будь-якому іншому відповідному законодавству Союзу, що передбачає видачу декларації про відповідність ЄС, зазначеної в статті 47;
5.	Якщо система штучного інтелекту передбачає обробку персональних даних, заява про те, що ця система штучного інтелекту відповідає Регламентам (ЄС) 2016/679 та (ЄС) 2018/1725 та Директиві (ЄС) 2016/680;
6.	Посилання на будь-які використані відповідні гармонізовані стандарти або будь-яку іншу загальну специфікацію, щодо якої заявляється відповідність;
7.	Де це застосовно, найменування та ідентифікаційний номер нотифікованого органу, опис виконаної процедури оцінки відповідності та ідентифікація виданого сертифіката;
8.	Місце та дата видачі декларації, прізвище та посада особи, яка її підписала, а також зазначення того, для кого або від імені кого ця особа підписала, підпис.

ДОДАТОК VI

Процедура оцінки відповідності на основі внутрішнього контролю

1.

Процедура оцінки відповідності на основі внутрішнього контролю є процедурою оцінки відповідності на основі пунктів 2, 3 та 4.

2.

Постачальник перевіряє, що встановлена система управління якістю відповідає вимогам статті 17.

3.

Постачальник вивчає інформацію, що міститься в технічній документації, з метою оцінки відповідності системи штучного інтелекту відповідним суттєвим вимогам, встановленим у главі III, розділі 2.

4.

Постачальник також перевіряє, що процес проєктування та розроблення системи штучного інтелекту та її постринковий моніторинг, зазначений у статті 72, відповідає технічній документації.

ДОДАТОК VII

Відповідність на основі оцінки системи управління якістю та оцінки технічної документації

1. Вступ

Відповідність на основі оцінки системи управління якістю та оцінки технічної документації є процедурою оцінки відповідності на основі пунктів 2–5.

2. Огляд

Затверджена система управління якістю для проєктування, розроблення та тестування систем штучного інтелекту відповідно до статті 17 перевіряється відповідно до пункту 3 та підлягає нагляду, як зазначено в пункті 5. Технічна документація системи штучного інтелекту перевіряється відповідно до пункту 4.

3. Система управління якістю

3.1. Заява постачальника включає:

(а) найменування та адресу постачальника та, якщо заява подається уповноваженим представником, також їхнє найменування та адресу;

(б) перелік систем штучного інтелекту, охоплених однією системою управління якістю;

(в) технічну документацію для кожної системи штучного інтелекту, охопленої однією

системою управління якістю;

(г) документацію щодо системи управління якістю, яка охоплює всі аспекти, перелічені в статті 17;

(д) опис процедур, що діють для забезпечення того, що система управління якістю залишається адекватною та ефективною;

(е) письмову заяву про те, що та сама заява не була подана до жодного іншого нотифікованого органу.

3.2. Система управління якістю оцінюється нотифікованим органом, який визначає, чи вона відповідає вимогам, зазначеним у статті 17.
Рішення доводиться до відома постачальника або його уповноваженого представника.

Повідомлення містить висновки оцінки системи управління якістю та обґрунтоване рішення про оцінку.

3.3. Схвалена система управління якістю продовжує впроваджуватись і підтримуватись постачальником таким чином, щоб вона залишалася адекватною та ефективною.

3.4. Будь-яка запланована зміна до затвердженої системи управління якістю або до переліку систем штучного інтелекту, охоплених останньою, доводиться до відома нотифікованого органу постачальником. Запропоновані зміни розглядаються нотифікованим органом, який вирішує, чи продовжує модифікована система управління якістю відповідати вимогам, зазначеним у пункті 3.2, або чи потрібна повторна оцінка.

Нотифікований орган повідомляє постачальника про своє рішення. Повідомлення містить висновки розгляду змін та обґрунтоване рішення про оцінку.

4. Контроль технічної документації.

4.1. На додаток до заяви, зазначеної в пункті 3, постачальник подає заяву до нотифікованого органу за своїм вибором для оцінки технічної документації, що стосується системи штучного інтелекту, яку постачальник має намір вивести на ринок або ввести в експлуатацію та яка охоплена системою управління якістю, зазначеною в пункті 3.

4.2. Заява включає:

(а) найменування та адресу постачальника ;

(б) письмову заяву про те, що та сама заява не була подана до жодного іншого нотифікованого органу;

(в) технічну документацію, зазначену в Додатку IV.

4.3. Технічна документація перевіряється нотифікованим органом. Де це доречно та в межах, необхідних для виконання його завдань, нотифікованому органу надається повний доступ до використаних наборів даних для навчання, валідації та тестування, включаючи, де це доцільно та з урахуванням гарантій безпеки, через API або інші відповідні технічні засоби та інструменти, що забезпечують віддалений доступ.

4.4. Під час розгляду технічної документації нотифікований орган може вимагати від постачальника надати додаткові докази або провести додаткові тести для належної оцінки відповідності системи штучного інтелекту вимогам, встановленим у главі III, розділі 2. Якщо нотифікований орган не задоволений тестами, проведеними постачальником,

нотифікований орган сам безпосередньо проводить відповідні тести, де це доречно.

4.5. Де це необхідно для оцінки відповідності високоризикової системи штучного інтелекту вимогам, встановленим у главі III, розділі 2, після того як усі інші розумні засоби перевірки відповідності були вичерпані та виявилися недостатніми, і за обґрунтованим запитом, нотифікованому органу також надається доступ до навчальних та навчених моделей системи штучного інтелекту, включаючи її відповідні параметри. Такий доступ підпадає під дію чинного законодавства Союзу про захист інтелектуальної власності та комерційної таємниці.

4.6. Рішення нотифікованого органу доводиться до відома постачальника або його уповноваженого представника. Повідомлення містить висновки оцінки технічної документації та обґрунтоване рішення про оцінку.
Якщо система штучного інтелекту відповідає вимогам, встановленим у главі III, розділі 2, нотифікований орган видає сертифікат оцінки технічної документації Союзу. Сертифікат містить найменування та адресу постачальника, висновки перевірки, умови (якщо такі є) його дійсності та дані, необхідні для ідентифікації системи штучного інтелекту.

Сертифікат та його додатки містять усю відповідну інформацію для можливості оцінки відповідності системи штучного інтелекту та для

можливості контролю системи штучного інтелекту під час її використання, де це застосовно.

Якщо система штучного інтелекту не відповідає вимогам, встановленим у главі III, розділі 2, нотифікований орган відмовляє у видачі сертифіката оцінки технічної документації Союзу та відповідним чином інформує заявника, надаючи детальні причини відмови.

Якщо система штучного інтелекту не відповідає вимогам щодо даних, що використовуються для її навчання, перед поданням заяви на нову оцінку відповідності потрібне повторне навчання системи штучного інтелекту. У такому випадку обґрунтоване рішення про оцінку нотифікованого органу про відмову у видачі сертифіката оцінки технічної документації Союзу містить конкретні міркування щодо якісних даних, використаних для навчання системи штучного інтелекту, зокрема щодо причин невідповідності.

4.7. Будь-яка зміна системи штучного інтелекту, яка може вплинути на відповідність системи штучного інтелекту вимогам або її призначення, оцінюється нотифікованим органом, який видав сертифікат оцінки технічної документації Союзу. Постачальник інформує такий нотифікований орган про свій намір внести будь-яку із зазначених вище змін або якщо він іншим чином дізнається про настання таких змін. Заплановані зміни оцінюються

нотифікованим органом, який вирішує, чи вимагають ці зміни нової оцінки відповідності відповідно до статті 43(4), або чи можуть вони бути вирішені шляхом доповнення до сертифіката оцінки технічної документації Союзу. В останньому випадку нотифікований орган оцінює зміни, повідомляє постачальника про своє рішення та, якщо зміни схвалені, видає постачальнику доповнення до сертифіката оцінки технічної документації Союзу.

5. Нагляд за затвердженою системою управління якістю.

5.1. Метою нагляду, здійснюваного нотифікованим органом, зазначеним у пункті 3, є забезпечення того, що постачальник належним чином дотримується умов та положень затвердженої системи управління якістю.

5.2. З метою оцінки постачальник надає нотифікованому органу доступ до приміщень, де здійснюється проєктування, розроблення, тестування систем штучного інтелекту. Постачальник також надає нотифікованому органу всю необхідну інформацію.

	5.3.	Нотифікований орган проводить періодичні аудити для переконання, що постачальник підтримує та застосовує систему управління якістю, та надає постачальнику звіт про аудит. У контексті цих аудитів нотифікований орган може проводити додаткові тести систем штучного інтелекту, для яких був виданий сертифікат оцінки технічної документації Союзу.

ДОДАТОК VIII

Інформація, що підлягає поданню при реєстрації високоризикових систем штучного інтелекту відповідно до статті 49

Розділ A — Інформація, що підлягає поданню постачальниками високоризикових систем штучного інтелекту відповідно до статті 49(1)

Щодо високоризикових систем штучного інтелекту, що підлягають реєстрації відповідно до статті 49(1), надається та надалі оновлюється така інформація:

1.	Найменування, адреса та контактні дані постачальника;
2.	Якщо подання інформації здійснюється іншою особою від імені постачальника, найменування, адреса та контактні дані цієї особи;
3.	Найменування, адреса та контактні дані уповноваженого представника, де це застосовно;
4.	Торгове найменування системи штучного інтелекту та будь-яке додаткове однозначне посилання, що дозволяє ідентифікацію та відстежуваність системи штучного інтелекту;
5.	Опис призначення системи штучного інтелекту та компонентів і функцій, що підтримуються цією системою штучного інтелекту;
6.	Базовий та стислий опис інформації, що використовується системою (дані, вхідні дані), та її операційна логіка;
7.	Статус системи штучного інтелекту (на ринку або в експлуатації; більше не виводиться на ринок / не використовується, відкликана);
8.	Тип, номер та дата закінчення терміну дії сертифіката, виданого нотифікованим органом, та найменування або ідентифікаційний номер цього нотифікованого органу, де це застосовно;
9.	Відскановану копію сертифіката, зазначеного в пункті 8, де це застосовно;
10.	Будь-які держави-члени, в яких система штучного інтелекту була виведена на ринок, введена в експлуатацію або надана до використання в Союзі;

11.	Копія декларації про відповідність ЄС, зазначена в статті 47;
12.	Електронні інструкції з використання; ця інформація не надається для високоризикових систем штучного інтелекту у сферах правоохоронної діяльності або міграції, притулку та управління прикордонним контролем, зазначених у Додатку III, пунктах 1, 6 та 7;
13.	URL для додаткової інформації (необов'язково).

Розділ B — Інформація, що підлягає поданню постачальниками високоризикових систем штучного інтелекту відповідно до статті 49(2)

Щодо систем штучного інтелекту, що підлягають реєстрації відповідно до статті 49(2), надається та надалі оновлюється така інформація:

1.	Найменування, адреса та контактні дані постачальника;
2.	Якщо подання інформації здійснюється іншою особою від імені постачальника, найменування, адреса та контактні дані цієї особи;
3.	Найменування, адреса та контактні дані уповноваженого представника, де це застосовно;
4.	Торгове найменування системи штучного інтелекту та будь-яке додаткове однозначне посилання, що дозволяє ідентифікацію та відстежуваність системи штучного інтелекту;
5.	Опис призначення системи штучного інтелекту;
6.	Умова або умови відповідно до статті 6(3), на основі яких система штучного інтелекту вважається такою, що не є високоризиковою;
7.	Короткий виклад підстав, на яких система штучного інтелекту вважається такою, що не є високоризиковою, при застосуванні процедури відповідно до статті 6(3);
8.	Статус системи штучного інтелекту (на ринку або в експлуатації; більше не виводиться на ринок / не використовується, відкликана);
9.	Будь-які держави-члени, в яких система штучного інтелекту була виведена на ринок, введена в експлуатацію або надана до

використання в Союзі.

Розділ C — Інформація, що підлягає поданню суб'єктами розгортання високоризикових систем штучного інтелекту відповідно до статті 49(3)

Щодо високоризикових систем штучного інтелекту, що підлягають реєстрації відповідно до статті 49(3), надається та надалі оновлюється така інформація:

1.	Найменування, адреса та контактні дані суб'єкта розгортання;
2.	Найменування, адреса та контактні дані особи, що подає інформацію від імені суб'єкта розгортання;
3.	URL запису системи штучного інтелекту в базі даних ЄС, здійсненого її постачальником;
4.	Стислий виклад висновків оцінки впливу на основні права, проведеної відповідно до статті 27;
5.	Стислий виклад оцінки впливу на захист даних, проведеної відповідно до статті 35 Регламенту (ЄС) 2016/679 або статті 27 Директиви (ЄС) 2016/680, як зазначено в статті 26(8) цього Регламенту, де це застосовно.

ДОДАТОК IX

Інформація, що підлягає поданню при реєстрації високоризикових систем штучного інтелекту, перелічених у Додатку III, стосовно тестування в реальних умовах відповідно до статті 60

Щодо тестування в реальних умовах, що підлягає реєстрації відповідно до статті 60, надається та надалі оновлюється така інформація:

1.	Єдиний унікальний ідентифікаційний номер тестування в реальних умовах у масштабах Союзу;
2.	Найменування та контактні дані постачальника або потенційного постачальника та суб'єктів розгортання, залучених до тестування в реальних умовах;
3.	Стислий опис системи штучного інтелекту, її призначення та іншої інформації, необхідної для ідентифікації системи;
4.	Стислий виклад основних характеристик плану тестування в реальних умовах;
5.	Інформація про призупинення або припинення тестування в реальних умовах.

ДОДАТОК X

Законодавчі акти Союзу щодо великомасштабних інформаційних систем у сфері свободи, безпеки та правосуддя

1. Шенгенська інформаційна система

(а)	Регламент (ЄС) 2018/1860 Європейського Парламенту та Ради від 28 листопада 2018 року про використання Шенгенської інформаційної системи для повернення незаконно перебуваючих громадян третіх країн (OJ L 312, 7.12.2018, p. 1).
(б)	Регламент (ЄС) 2018/1861 Європейського Парламенту та Ради від 28 листопада 2018 року про створення, функціонування та використання Шенгенської інформаційної системи (SIS) у сфері прикордонного контролю, внесення змін до Конвенції про впровадження Шенгенської угоди, внесення змін та скасування Регламенту (ЄС) № 1987/2006 (OJ L 312, 7.12.2018, p. 14).
(в)	Регламент (ЄС) 2018/1862 Європейського Парламенту та Ради від 28 листопада 2018 року про створення, функціонування та використання Шенгенської інформаційної системи (SIS) у сфері поліцейського співробітництва та судового співробітництва у кримінальних справах, внесення змін та скасування Рішення Ради 2007/533/ПВД та скасування Регламенту (ЄС) № 1986/2006 Європейського Парламенту та Ради та Рішення Комісії 2010/261/ЄС (OJ L 312, 7.12.2018, p. 56).

2. Візова інформаційна система

(а)	Регламент (ЄС) 2021/1133 Європейського Парламенту та Ради від 7 липня 2021 року про внесення змін до Регламентів (ЄС) № 603/2013, (ЄС) 2016/794, (ЄС) 2018/1862, (ЄС) 2019/816 та (ЄС) 2019/818 щодо встановлення умов для доступу до інших інформаційних систем ЄС для цілей Візової інформаційної системи (OJ L 248, 13.7.2021, p. 1).
(б)	Регламент (ЄС) 2021/1134 Європейського Парламенту та Ради від 7 липня 2021 року про внесення змін до Регламентів (ЄС) № 767/2008, (ЄС) № 810/2009, (ЄС) 2016/399, (ЄС) 2017/2226,

(ЄС) 2018/1240, (ЄС) 2018/1860, (ЄС) 2018/1861, (ЄС) 2019/817 та (ЄС) 2019/1896 Європейського Парламенту та Ради та скасування Рішень Ради 2004/512/ЄС та 2008/633/ПВД з метою реформування Візової інформаційної системи (OJ L 248, 13.7.2021, p. 11).

3. Eurodac

Регламент (ЄС) 2024/1358 Європейського Парламенту та Ради від 14 травня 2024 року про створення 'Eurodac' для порівняння біометричних даних з метою ефективного застосування Регламентів (ЄС) 2024/1315 та (ЄС) 2024/1350 Європейського Парламенту та Ради та Директиви Ради 2001/55/ЄС і для ідентифікації незаконно перебуваючих громадян третіх країн та осіб без громадянства, а також про запити на порівняння з даними Eurodac правоохоронними органами держав-членів та Europol з правоохоронною метою, внесення змін до Регламентів (ЄС) 2018/1240 та (ЄС) 2019/818 Європейського Парламенту та Ради та скасування Регламенту (ЄС) № 603/2013 Європейського Парламенту та Ради (OJ L, 2024/1358, 22.5.2024, ELI: http://data.europa.eu/eli/reg/2024/1358/oj).

4. Система в'їзду/виїзду

Регламент (ЄС) 2017/2226 Європейського Парламенту та Ради від 30 листопада 2017 року про створення Системи в'їзду/виїзду (EES) для реєстрації даних в'їзду та виїзду та даних про відмову у в'їзді громадян третіх країн, які перетинають зовнішні кордони держав-членів, та визначення умов доступу до EES з правоохоронною метою, а також внесення змін до Конвенції про впровадження Шенгенської угоди та Регламентів (ЄС) № 767/2008 та (ЄС) № 1077/2011 (OJ L 327, 9.12.2017, p. 20).

5. Європейська система інформації та авторизації подорожей

(а) Регламент (ЄС) 2018/1240 Європейського Парламенту та Ради від 12 вересня 2018 року про створення Європейської системи інформації та авторизації подорожей (ETIAS) та внесення змін до Регламентів (ЄС) № 1077/2011, (ЄС) № 515/2014, (ЄС) 2016/399, (ЄС) 2016/1624 та (ЄС) 2017/2226 (OJ L 236, 19.9.2018, p. 1).

(б) Регламент (ЄС) 2018/1241 Європейського Парламенту та Ради від 12 вересня 2018 року про внесення змін до Регламенту (ЄС) 2016/794 з метою створення Європейської системи інформації та авторизації подорожей (ETIAS) (OJ L 236, 19.9.2018, p. 72).

6. Європейська інформаційна система судимостей стосовно громадян третіх країн та осіб без громадянства

Регламент (ЄС) 2019/816 Європейського Парламенту та Ради від 17 квітня 2019 року про створення централізованої системи для ідентифікації держав-членів, що зберігають інформацію про засудження громадян третіх країн та осіб без громадянства (ECRIS-TCN), з метою доповнення Європейської інформаційної системи судимостей та внесення змін до Регламенту (ЄС) 2018/1726 (OJ L 135, 22.5.2019, p. 1).

7. Сумісність

(а)	Регламент (ЄС) 2019/817 Європейського Парламенту та Ради від 20 травня 2019 року про створення рамок для сумісності між інформаційними системами ЄС у сфері кордонів та віз та внесення змін до Регламентів (ЄС) № 767/2008, (ЄС) 2016/399, (ЄС) 2017/2226, (ЄС) 2018/1240, (ЄС) 2018/1726 та (ЄС) 2018/1861 Європейського Парламенту та Ради та Рішень Ради 2004/512/ЄС та 2008/633/ПВД (OJ L 135, 22.5.2019, p. 27).
(б)	Регламент (ЄС) 2019/818 Європейського Парламенту та Ради від 20 травня 2019 року про створення рамок для сумісності між інформаційними системами ЄС у сфері поліцейського та судового співробітництва, притулку та міграції та внесення змін до Регламентів (ЄС) 2018/1726, (ЄС) 2018/1862 та (ЄС) 2019/816 (OJ L 135, 22.5.2019, p. 85).

ДОДАТОК XI

Технічна документація, зазначена в статті 53(1), пункті (a) — технічна документація для постачальників моделей штучного інтелекту загального призначення

Розділ 1

Інформація, що підлягає наданню всіма постачальниками моделей штучного інтелекту загального призначення

Технічна документація, зазначена в статті 53(1), пункті (a), містить щонайменше таку інформацію, що відповідає розміру та профілю ризику моделі:

1. Загальний опис моделі штучного інтелекту загального призначення, включаючи:

   (a) завдання, які модель призначена виконувати, та тип і характер систем штучного інтелекту, до яких вона може бути інтегрована;

   (б) застосовні політики допустимого використання;

   (в) дата випуску та методи розповсюдження;

   (г) архітектура та кількість параметрів;

   (д) модальність (наприклад, текст, зображення) та формат вхідних і вихідних даних;

   (е) ліцензія.

2. Детальний опис елементів моделі, зазначених у пункті 1, та відповідна інформація про процес розроблення, включаючи такі елементи:

   (a) технічні засоби (наприклад, інструкції з використання, інфраструктура,

інструменти), необхідні для інтеграції моделі штучного інтелекту загального призначення в системи штучного інтелекту;

(б) технічні вимоги до моделі та процесу навчання, включаючи методології та методи навчання, ключові проєктні рішення, включаючи обґрунтування та зроблені припущення; для оптимізації чого призначено модель та значущість різних параметрів, де це застосовно;

(в) інформація про дані, використані для навчання, тестування та валідації, де це застосовно, включаючи тип та походження даних і методології куратування (наприклад, очищення, фільтрація тощо), кількість точок даних, їхній обсяг та основні характеристики; яким чином дані були отримані та відібрані, а також всі інші заходи для виявлення непридатності джерел даних та методи виявлення ідентифікованих упереджень, де це застосовно;

(г) обчислювальні ресурси, використані для навчання моделі

(наприклад, кількість операцій з плаваючою комою), час навчання та інші відповідні деталі, пов'язані з навчанням;

(д) відоме або приблизне енергоспоживання моделі.

Стосовно пункту (е), якщо енергоспоживання моделі невідоме, енергоспоживання може базуватися на інформації про використані обчислювальні ресурси.

Розділ 2

Додаткова інформація, що підлягає наданню постачальниками моделей штучного інтелекту загального призначення із системним ризиком

1. Детальний опис стратегій оцінки, включаючи результати оцінки, на основі наявних публічних протоколів і інструментів оцінки або іншим чином інших методологій оцінки. Стратегії оцінки включають критерії оцінки, метрики та методологію виявлення обмежень.

2. Де це застосовно, детальний опис заходів, вжитих з метою проведення внутрішнього та/або зовнішнього тестування на стійкість до атак (наприклад, red teaming), адаптацій моделі, включаючи вирівнювання та тонке настроювання.

3. Де це застосовно, детальний опис архітектури системи, що пояснює, яким чином програмні компоненти будуються один на одному або взаємодіють між собою та інтегруються в загальну обробку.

ДОДАТОК XII

Інформація щодо прозорості, зазначена в статті 53(1), пункті (b) — технічна документація для постачальників моделей штучного інтелекту загального призначення для нижчих за потоком постачальників, що інтегрують модель у свою систему штучного інтелекту

Інформація, зазначена в статті 53(1), пункті (b), містить щонайменше таке:

1. Загальний опис моделі штучного інтелекту загального призначення, включаючи:

(а) завдання, які модель призначена виконувати, та тип і характер систем штучного інтелекту, до яких вона може бути інтегрована;

(б) застосовні політики допустимого використання;

(в) дата випуску та методи розповсюдження;

(г) яким чином модель взаємодіє або може використовуватися для взаємодії з апаратним або програмним забезпеченням, що не є частиною самої моделі, де це застосовно;

(д) версії відповідного програмного забезпечення, пов'язаного з використанням моделі штучного інтелекту загального призначення, де це застосовно;

(е) архітектура та кількість параметрів;

(є) модальність (наприклад, текст, зображення) та формат вхідних і вихідних даних;

(ж) ліцензія для моделі.

2. Опис елементів моделі та процесу її розроблення, включаючи:

(а) технічні засоби (наприклад, інструкції з використання, інфраструктура, інструменти), необхідні для інтеграції моделі штучного інтелекту загального призначення в системи штучного інтелекту;

(б) модальність (наприклад, текст, зображення тощо) та формат вхідних і вихідних даних та їхній максимальний розмір (наприклад, довжина контекстного вікна тощо);

(в) інформація про дані, використані для навчання, тестування та валідації, де це застосовно, включаючи тип та походження даних і методології куратування.

ДОДАТОК XIII

Критерії для визначення моделей штучного інтелекту загального призначення із системним ризиком, зазначені в статті 51

З метою визначення того, що модель штучного інтелекту загального призначення має можливості або вплив, еквівалентні тим, що встановлені в статті 51(1), пункті (a), Комісія враховує такі критерії:

(а)	кількість параметрів моделі;
(б)	якість або розмір набору даних, наприклад, виміряний через токени;
(в)	обсяг обчислень, використаних для навчання моделі, виміряний у операціях з плаваючою комою або позначений комбінацією інших змінних, таких як приблизна вартість навчання, приблизний час, необхідний для навчання, або приблизне енергоспоживання для навчання;
(г)	вхідні та вихідні модальності моделі, такі як текст у текст (великі мовні моделі), текст у зображення, мультимодальність, та сучасні порогові значення для визначення можливостей з високим впливом для кожної модальності та конкретний тип вхідних і вихідних даних (наприклад, біологічні послідовності);
(д)	контрольні показники та оцінки можливостей моделі, включаючи врахування кількості завдань без додаткового навчання, здатності до адаптації до вивчення нових, відмінних завдань, її рівня автономії та масштабованості, інструментів, до яких вона має доступ;
(е)	чи має вона значний вплив на внутрішній ринок завдяки своєму охопленню, що вважається презумпцією, коли вона була надана щонайменше 10 000 зареєстрованим бізнес-користувачам, заснованим у Союзі;
(є)	кількість зареєстрованих кінцевих користувачів.

ELI: http://data.europa.eu/eli/reg/2024/1689/oj

ISSN 1977-0677 (electronic edition)

Кінець документа · Adopta · https://adopta.com.ua/eu-ai-act-uk.html