

Становище на Комитета (член 64)



Становище 28/2024 относно някои аспекти на защитата на данните, свързани с обработването на лични данни в рамките на моделите на ИИ

Прието на 17 декември 2024 г.

Резюме

Технологиите в сферата на изкуствения интелект (ИИ) създават много възможности и ползи в широк спектър от сектори и социални дейности.

Като защитава основното право на защита на данните, Общият регламент относно защитата на данните (ОРЗД) подкрепя тези възможности и насърчава други основни права на ЕС, включително правото на свобода на мисълта, на изразяване на мнение и на информация, правото на образование или свободата на стопанска инициатива. По този начин ОРЗД представлява правна рамка, която насърчава отговорните иновации.

В този смисъл, като взе предвид въпросите, свързани със защитата на данните, които тези технологии повдигат, ирландският надзорен орган поиска от Европейския комитет по защита на данните (ЕКЗД) да издаде становище по въпроси с общо приложение съгласно член 64, параграф 2 от ОРЗД. Искането се отнася до обработването на лични данни на етапите на разработване и внедряване на моделите на изкуствен интелект („ИИ“). По-специално искането се отнася до това: 1) кога и как даден модел на ИИ може да се счита за „анонимен“; 2) как администраторите могат да докажат уместността на легитимния интерес като правно основание на етапите на разработване и 3) внедряване; и 4) какви са последиците от незаконосъобразното обработване на лични данни на етапа на разработване на модел на ИИ за последващото обработване или функциониране.

По отношение на първия въпрос в становището се споменава, че твърденията за анонимност на даден модел на ИИ следва да се оценяват от компетентните надзорни органи (НО) за всеки отделен случай, тъй като ЕКЗД счита, че моделите на ИИ, обучени с лични данни, не могат да се считат за анонимни във всички случаи. За да може даден модел с изкуствен интелект да се счита за анонимен, както 1) вероятността за пряко (включително вероятно) извличане на лични данни по отношение на лицата, чиито лични данни са били използвани за разработването на модела, така и 2) вероятността за получаване, умишлено или не, на такива лични данни от запитвания, следва да бъде незначителна, като се вземат предвид *„всички средства, за които има достатъчна вероятност да бъдат използвани“* от администратора или друго лице.

За да извършат своята оценка, НО следва да прегледат документацията, предоставена от администратора, за да докажат анонимността на модела. В това отношение в становището се съдържа незадължителен и неизчерпателен списък на методите, които администраторите може да използват при доказване на анонимността и които следователно НО може да вземат предвид при оценяване на твърдението на администратора за анонимност. Това включва например подходите, възприети от администраторите по време на етапа на разработване, за предотвратяване или ограничаване на събирането на лични данни, използвани за обучение, за намаляване на тяхната възможност за идентификация, за предотвратяване на тяхното извличане или за предоставяне на увереност относно най-съвременната устойчивост на атаки.

По отношение на втория и третия въпрос в становището се съдържат общи съображения, които НО да вземат под внимание, когато преценяват дали администраторите могат да разчитат на легитимен интерес като подходящо правно основание за обработване, извършвано в рамките на разработването и внедряването на модели на ИИ.

В становището се припомня, че между предвидените в ОРЗД правни основания не съществува йерархия и че администраторите са тези, които трябва да определят подходящото правно

основание за своите дейности по обработване. След това в становището се припомня тестът, състоящ се от три стъпки, който следва да се извърши при оценката на използването на легитимен интерес като правно основание, т.е. 1) установяване на легитимния интерес на администратора или на трета страна; 2) анализиране на необходимостта от обработването за целите на легитимния(те) интерес(и) (наричан още „критерий за необходимост“), и 3) оценка на това дали над легитимния(те) интерес(и) не надделява(т) интересите или основните права и свободи на субектите на данни (наричан още „сравнителен тест“).

Що се отнася до първата стъпка, в становището се припомня, че даден интерес може да се счита за законен, ако са изпълнени следните три кумулативни критерия: интересът 1) е законен; 2) е ясно и точно формулиран; и 3) е реален и актуален (т.е. не спекулативен). Такъв интерес може да обхваща например, в разработването на модел на ИИ — разработване на услугата на агент за разговор за подпомагане на потребителите, или във внедряването на такъв — подобряване на откриването на заплахи в информационна система.

Що се отнася до втората стъпка, в становището се припомня, че оценката на необходимостта предполага да се прецени: 1) дали дейността по обработване на данни ще даде възможност за преследване на легитимния интерес; и 2) дали няма по-малко инвазивен начин за преследване на този интерес. Когато преценяват дали е изпълнено условието за необходимост, компетентните органи следва да обърнат специално внимание на обема на обработваните лични данни и дали той е пропорционален на преследването на въпросния легитимен интерес, също и с оглед на принципа за свеждане на данните до минимум.

Що се отнася до третата стъпка, в становището се припомня, че сравнителният тест следва да се извършва, като се вземат предвид конкретните обстоятелства във всеки отделен случай. След това се прави преглед на елементите, които НО може да вземат предвид, когато преценяват дали интересът на администратора или на трета страна е по-силен от интересите, основните права и свободи на субектите на данни.

Като част от третата стъпка, в становището се подчертават конкретни рискове за основните права, които могат да възникнат или на етапа на разработване, или на етапа на внедряване на моделите на ИИ. В него също така се пояснява, че обработването на лични данни, което се извършва по време на етапите на разработване и внедряване на модели на ИИ, може да окаже въздействие върху субектите на данни по различни начини, които могат да бъдат положителни или отрицателни. За да оценят това въздействие, НО може да вземат предвид естеството на данните, обработвани от моделите, контекста на обработването и възможните по-нататъшни последици от него.

Освен това в становището се подчертава ролята на разумните очаквания на субектите на данни в сравнителния тест. Това може да бъде важно поради сложността на технологиите, използвани в моделите на ИИ, и поради факта, че за физическите лица може да е трудно да разберат разнообразието на техните потенциални употреби, както и на различните свързани дейности по обработване. В това отношение както информацията, предоставена на субектите на данни, така и контекстът на обработването могат да бъдат сред елементите, които трябва да се вземат предвид, за да се прецени дали лицата могат с основание да очакват, че техните лични данни ще бъдат обработвани. По отношение на контекста това може да включва: дали личните данни са били публично достъпни или не, естеството на отношенията между субекта на данните и администратора (и дали съществува връзка между тях), естеството на услугата, контекста, в който са събрани личните данни, източника, от който са събрани данните (т.е. уебсайта или услугата, където са събрани личните данни, и настройките за поверителност, които те предлагат),

потенциалното по-нататъшно използване на модела и дали субектите на данни всъщност знаят, че личните им данни са онлайн.

В становището също така се припомня, че когато интересите, правата и свободите на субектите на данни изглежда надделяват над легитимните интереси на администратора или на трета страна, администраторът може да обмисли въвеждането на смекчаващи мерки за ограничаване на въздействието на обработването върху тези физически лица. Смекчаващите мерки не следва да се бъркат с мерките, които администраторът по закон е задължен да приеме така или иначе, за да гарантира спазването на ОРЗД. Освен това мерките следва да бъдат съобразени с обстоятелствата по случая и характеристиките на модела на ИИ, включително неговото предназначение. В това отношение в становището се предоставя неизчерпателен списък с примери за смекчаващи мерки във връзка с етапа на разработване (също и по отношение на извличането на данни от интернет) и етапа на внедряване. Смекчаващите мерки може да претърпяват бързо развитие и следва да бъдат съобразени с обстоятелствата по случая. Поради това НО са тези, които трябва да оценяват за всеки отделен случай целесъобразността на приложените смекчаващи мерки.

Що се отнася до четвъртия въпрос, в становището като цяло се припомня, че НО разполагат с правомощия да оценяват възможното(ите) нарушение(я) и да избират подходящи, необходими и пропорционални мерки, като вземат предвид обстоятелствата във всеки отделен случай. След това в становището се разглеждат три сценария.

При сценарий 1 личните данни се съхраняват в модела на ИИ (което означава, че моделът не може да се счита за анонимен, както е описано в първия въпрос) и впоследствие се обработват от същия администратор (например в рамките на внедряването на модела). В становището се посочва, че това дали етапите на разработване и внедряване включват отделни цели (и следователно представляват отделни дейности по обработване) и степента, до която липсата на правно основание за първоначалната дейност по обработване оказва въздействие върху законосъобразността на последващото обработване, следва да се оценява за всеки отделен случай, в зависимост от спецификата на случая.

При сценарий 2 личните данни се съхраняват в модела и се обработват от друг администратор в рамките на внедряването на модела. В тази връзка в становището се посочва, че НО следва да вземат предвид това, дали администраторът, който внедрява модела, е извършил подходяща оценка като част от задълженията си за отчетност, за да докаже спазването на член 5, параграф 1, буква а) и член 6 от ОРЗД, за да се увери, че моделът на ИИ не е разработен чрез незаконосъобразно обработване на лични данни. В тази оценка следва да се вземе предвид например източника на личните данни и дали при обработването на етапа на разработване е било констатирано нарушение, особено ако то е било установено от НО или от съда, като оценката следва да бъде по-малко или повече подробна в зависимост от рисковете, породени от обработването на етапа на внедряване.

Съгласно сценарий 3 администраторът незаконосъобразно обработва лични данни с цел разработването на модела на ИИ, след което гарантира, че те са анонимизирани, преди същият или друг администратор да започне друго обработване на лични данни в рамките на внедряването. В това отношение в становището се посочва, че ако може да се докаже, че последващото функциониране на модела на ИИ не включва обработването на лични данни, ЕКЗД счита, че ОРЗД няма да се прилага. Следователно, незаконосъобразността на първоначалното обработване не следва да оказва въздействие върху последващото функциониране на модела. Освен това ЕКЗД счита, че когато впоследствие администраторите

обработват лични данни, събрани по време на етапа на внедряване, след като моделът е анонимизиран, ОРЗД ще се прилага по отношение на тези операции по обработване. В тези случаи в становището се изтъква, че що се отнася до ОРЗД, законосъобразността на обработването, извършвано на етапа на внедряване, не следва да бъде засегната от незаконосъобразността на първоначалното обработване.

Съдържание

1	Въведение	7
1.1	Кратко изложение на фактите	7
1.2	Допустимост на искането за становище по член 64, параграф 2 от ОРЗД	9
2	Обхват и основни понятия	10
2.1	Приложно поле на становището	10
2.2	Основни понятия	12
2.3	Моделите на ИИ в рамките на становището	13
3	По съществото на искането	14
3.1	По съществото на моделите на ИИ във връзка с определението за лични данни	14
3.2	Относно обстоятелствата, при които моделите на ИИ биха могли да се считат за анонимни, и свързаните с тях доказателства	16
3.2.1	Общо съображение относно анонимизацията в разглеждания контекст	17
3.2.2	Елементи за оценка на остатъчната вероятност за идентифициране	19
3.3	Относно целесъобразността на легитимния интерес като правно основание за обработване на лични данни в контекста на разработването и внедряването на модели на ИИ	22
3.3.1	Общи коментари	23
3.3.2	Съображения относно трите стъпки на оценката на легитимния интерес при разработването и внедряването на модели на ИИ	25
3.4	Относно възможното въздействие на незаконосъобразното обработване при разработването на модел на ИИ върху законосъобразността на последващото обработване или експлоатация на модела на ИИ	36
3.4.1	Сценарий 1. Администратор обработва лични данни незаконно, за да разработи модела, личните данни се запазват в модела и впоследствие се обработват от същия администратор (например при внедряването на модела)	38
3.4.2	Сценарий 2. Администратор обработва лични данни незаконно, за да разработи модела, личните данни се запазват в модела и се обработват от друг администратор при внедряването на модела	39
3.4.3	Сценарий 3. Администраторът незаконно обработва лични данни, за да разработи модела, след което гарантира, че те са анонимизирани, преди същият или друг администратор да започне друго обработване на лични данни в рамките на внедряването	40
4	Заключителни бележки	41

Европейският комитет по защита на данните,

като взе предвид член 63 и член 64, параграф 2 от Регламент 2016/679/ЕС на Европейския парламент и на Съвета от 27 април 2016 г. относно защитата на физическите лица във връзка с обработването на лични данни и относно свободното движение на такива данни и за отмяна на Директива 95/46/ЕО (наричан по-нататък „ОРЗД“),

като взе предвид Споразумението за Европейското икономическо пространство, и по-специално приложение XI и протокол 37 към него, както е изменено с Решение на Съвместния комитет на ЕИП 154/2018 от 6 юли 2018 г.¹,

като взе предвид членове 10 и 22 от своя Правилник за дейността,

като има предвид, че:

(1) Главната роля на Европейския комитет по защита на данните (наричан по-нататък **„Комитетът“** или **„ЕКЗД“**) е да гарантира съгласуваното прилагане на ОРЗД в цялото Европейско икономическо пространство (**„ЕИП“**). В член 64, параграф 2 от ОРЗД се предвижда, че всеки надзорен орган (**„НО“**), председателят на Комитета или Комисията може да поиска всеки въпрос с общо приложение или с последици в повече от една държава членка на ЕИП, да бъде разгледан от Комитета с цел получаване на становище. Целта на настоящото становище е да се проучи въпрос с общо приложение или с последици в повече от една държава членка на ЕИП.

(2) Становището на Комитета следва да се приеме съгласно член 64, параграф 3 от ОРЗД във връзка с член 10, параграф 2 от Правилника за дейността на ЕКЗД в рамките на осем седмици от първия работен ден, след като председателят и компетентният надзорен орган установи, че досието е пълно. По решение на председателя този срок може да бъде удължен с още шест седмици поради сложното естество на въпроса.

ПРИЕ СЛЕДНОТО СТАНОВИЩЕ

1 Въведение

1.1 Кратко изложение на фактите

1. На 4 септември 2024 г. ирландският надзорен орган (**„НО на Ирландия“** или **„отправлящ искането НО“**) поиска от ЕКЗД да издаде становище съгласно член 64, параграф 2 от ОРЗД във връзка с моделите на ИИ и обработването на лични данни (**„Искането“**).
2. На 13 септември 2024 г. председателят на Комитета и НО на Ирландия приеха, че досието е пълно. На следващия работен ден, 16 септември 2024 г., досието е излъчено от секретариата на ЕКЗД. Като взе предвид сложността на въпроса, председателят на Комитета реши да удължи законоустановения срок в съответствие с член 64, параграф 3 от ОРЗД и член 10, параграф 4 от Правилника за дейността на ЕКЗД.

¹ Позоваванията на „държави членки“ в настоящото становище следва да се разбират като позовавания на „държавите — членки на ЕИП“. Позоваванията на „Съюза“ в настоящото становище следва да се разбират като позовавания на „ЕИП“.

3. Искането се отнася до някои елементи от обучението, актуализирането, разработването и експлоатацията на модели на ИИ, при които личните данни са част от съответния набор от данни. НО на Ирландия подчертава, че искането се отнася до ключови въпроси, които имат голямо въздействие върху субектите на данни и администраторите в ЕИП, и че на този етап няма хармонизирана позиция сред националните НО². Терминологията, която ще бъде използвана за целите на настоящото становище, е представена в раздели 2.2 и 2.3 по-долу.

4. НО на Ирландия зададе следните въпроси:

Въпрос 1: Счита ли се, че окончателният модел на ИИ, който е бил обучен с помощта на лични данни, във всички случаи не отговаря на определението за лични данни (както е посочено в член 4, параграф 1 от ОРЗД)?

Ако отговорът на първия въпрос е утвърдителен:

- i. На какъв етап от операциите по обработване, водещи до модел на ИИ, вече не се обработват лични данни?
 - а) Как може да се докаже, че моделът на ИИ не обработва лични данни?
- ii. Има ли фактори, поради които функционирането на окончателния модел на ИИ ще спре да се счита за анонимно?
 - а) Ако това е така, как могат да бъдат доказани предприетите мерки за смекчаване, предотвратяване или защита срещу тези фактори (за да се гарантира, че моделът на ИИ не обработва лични данни)?

Ако отговорът на първия въпрос е отрицателен:

- i. Какви са обстоятелствата, при които това може да се случи?
 - а) Ако това е така, как могат да бъдат доказани предприетите стъпки, за да се гарантира, че моделът на ИИ не обработва лични данни?

Въпрос 2: Когато администратор на данни разчита на легитимни интереси като правно основание за обработване на лични данни с цел създаване, актуализиране и/или разработване на модел на ИИ, как този администратор следва да докаже уместността на легитимните интереси като правно основание по отношение на обработването както на данни от трети страни, така и на данни от първа ръка?

- i. Какви съображения следва да вземе предвид администраторът, за да гарантира, че интересите на субектите на данни, чиито лични данни се обработват, са подходящо претеглени спрямо интересите на този администратор при:
 - а) Данни от трети страни
 - б) Данни от първа ръка

Въпрос 3: След обучението, когато администратор на данни разчита на легитимни интереси като правно основание за обработването на лични данни, което се извършва в рамките на модел на

² Искане, стр. 1.

ИИ или система с ИИ, от която моделът на ИИ е част, как администраторът трябва да докаже уместността на легитимните интереси като правно основание?

Въпрос 4: Ако е установено, че даден модел на ИИ е създаден, актуализиран или разработен с помощта на незаконосъобразно обработени лични данни, какво е въздействието на това, ако има такова, върху законосъобразността на продължаващото или последващото обработване или функциониране на модела на ИИ, самостоятелно или като част от система с ИИ, когато:

- i. Моделът на ИИ, самостоятелно или като част от система с ИИ, обработва лични данни?
- ii. Нито моделът на ИИ, нито моделът на ИИ като част от система с ИИ обработва лични данни?

1.2 Допустимост на искането за становище по член 64, параграф 2 от ОРЗД

- 5. В член 64, параграф 2 от ОРЗД се предвижда, по-специално, че всеки НО може да поиска всеки въпрос с общо приложение или с последици в повече от една държава членка на ЕИП, да бъде разгледан от Комитета с цел получаване на становище.
- 6. Отправлящият искането НО зададе въпроси към ЕКЗД относно аспектите на защитата на данните в рамките на моделите на ИИ. В искането се уточнява, че макар много организации вече да използват модели на ИИ, включително големи езикови модели („LLM“), тяхното функциониране, обучение и използване поражда *„редица широкообхватни опасения, свързани със защитата на данните“*³, които *„засягат субектите на данни в целия ЕС/ЕИП“*⁴.
- 7. В искането по същество се повдигат въпроси относно i) прилагането на понятието за лични данни; ii) принципа на законосъобразност, с оглед, по-специално, на правното основание за легитимен интерес в рамките на моделите на ИИ; както и относно iii) последиците от незаконосъобразното обработване на лични данни на етапа на разработване на модели на ИИ върху последващото обработване или функциониране на модела.
- 8. Комитетът счита, че искането се отнася до *„въпрос с общо приложение“* по смисъла на член 64, параграф 2 от ОРЗД. По-специално въпросът е свързан с тълкуването и прилагането на член 4, параграф 1, член 5, параграф 1, буква а) и член 6 от ОРЗД във връзка с обработването на лични данни при разработването и внедряването на модели на ИИ. Както бе подчертано от отправящия искането НО, прилагането на тези разпоредби към моделите на ИИ повдига системни, абстрактни и нови въпроси⁵. Бързото разработване и внедряване на модели на ИИ от все повече организации повдига специфични въпроси и, както се посочва в искането, *„ЕКЗД ще има голяма полза от постигането на обща позиция по въпросите, повдигнати в настоящото искане, тъй като тези въпроси са от основно значение за планираната работа на ЕКЗД в краткосрочен и средносрочен план“*⁶. Освен това технологиите в сферата на ИИ създават много възможности и ползи в широк спектър от сектори и социални дейности. Освен това ОРЗД е правна рамка, която насърчава отговорните иновации. От това следва, че е налице общ интерес

³ Искане, стр. 1.

⁴ Пак там.

⁵ Искане, стр. 2.

⁶ Искане, стр. 1. Както е посочено в работната програма на ЕКЗД за 2024—2025 г., приета на 8 октомври 2024 г., достъпна на адрес https://www.edpb.europa.eu/system/files/2024-10/edpb_work_programme_2024-2025_en.pdf, ЕКЗД планира да издаде, *inter alia*, насоки относно анонимизацията, псевдонимизацията и извличането на данни в контекста на генеративния ИИ.

от извършването на тази оценка под формата на становище на ЕКЗД, за да се гарантира последователното прилагане на някои разпоредби на ОРЗД в рамките на моделите на ИИ.

9. Второто условие, посочено в член 64, параграф 2 от ОРЗД касае въпроси „с въздействие в повече от една държава членка“. ЕКЗД припомня, че терминът „въздействие“ следва да се тълкува *lato sensu* и следователно не се ограничава само до правни въздействия⁷. Тъй като все повече модели на ИИ се обучават и използват от все по-голям брой организации в ЕИП, те оказват въздействие върху голям брой субекти на данни в цялото ЕИП, някои от които вече са изразили опасения пред компетентния НО⁸. Поради това ЕКЗД счита, че въпросът, повдигнат от отправящия искането НО, също отговаря на това условие.
10. Искането включва писмена аргументация относно предисторията и мотивите за отправяне на въпросите към Комитета, включително относно съответната правна рамка. Поради това Комитетът счита, че искането е обосновано в съответствие с член 10, параграф 3 от Правилника за дейността на ЕКЗД.
11. В съответствие с член 64, параграф 3 от ОРЗД⁹ ЕКЗД не издава становище, ако вече е издавал такова по въпроса. Комитетът не е изготвил становище по същия въпрос и все още не е предоставил отговори на въпросите, произтичащи от искането.
12. Поради тези причини Комитетът счита, че искането е допустимо, и произтичащите от него въпроси следва да бъдат анализирани в настоящото становище („Становището“), прието съгласно член 64, параграф 2 от ОРЗД.

2 Обхват и основни понятия

2.1 Приложно поле на становището

13. Комитетът е съгласен с отправящия искането НО, че от гледна точка на защитата на данните разработването и внедряването на модели на ИИ поражда основни въпроси, свързани със защитата на данните. Въпросите се отнасят по-специално до: i) това кога и как даден модел на ИИ може да се счита за „анонимен“ (въпрос 1 от искането); ii) как администраторите могат да докажат целесъобразността на легитимния интерес като правно основание на етапите на разработване (въпрос 2 от искането) и внедряване (въпрос 3 от искането); и iii) дали незаконосъобразното обработване на лични данни на етапа на разработване има последици за законосъобразността на последващото обработване или експлоатация на модела на ИИ (въпрос 4 от искането).
14. ЕКЗД припомня, че надзорните органи отговарят за наблюдението на прилагането на ОРЗД и следва да допринасят за неговото последователно прилагане в целия Съюз¹⁰. Поради това е в рамките на компетентността на надзорните органи да проучват конкретни модели на ИИ и в рамките на това проучване да извършват оценки за всеки отделен случай.

⁷ ЕКЗД, Вътрешен документ 3/2019 относно вътрешни насоки по член 64, параграф 2 от ОРЗД, приет на 8 октомври 2019 г., параграф 15, на разположение на https://www.edpb.europa.eu/system/files/2022-07/internaledpb_document_201903_art64.2_en.pdf.

⁸ Искане, стр. 1—2.

⁹ Член 64, параграф 3 от ОРЗД и член 10, параграф 4 от Правилника за дейността на ЕКЗД.

¹⁰ Член 51, параграф 1 от ОРЗД и член 51, параграф 2 от ОРЗД.

15. Настоящото становище предоставя рамка, с чиято помощ компетентните НО да оценяват конкретни случаи, в които биха възникнали (някои от) въпросите, повдигнати в искането. Настоящото становище няма за цел да бъде изчерпателно, а по-скоро да представя общи съображения относно тълкуването на съответните разпоредби, които компетентните надзорни органи следва да вземат предвид в максимална степен, когато използват правомощията си за разследване. Въпреки че настоящото становище е отправено до компетентните надзорни органи и се отнася до техните дейности и правомощия, то не накърнява задълженията на администраторите и обработващите лични данни съгласно ОРЗД. По-специално, в съответствие с принципа на отчетност, заложен в член 5, параграф 2 от ОРЗД, администраторите носят отговорност и са в състояние да докажат спазването на всички принципи, свързани с обработването на лични данни от тяхна страна.
16. В някои случаи в становището може да са представени някои примери, но като се има предвид широкият обхват на въпросите, включени в искането, както и различните видове модели на ИИ, обхванати в него, в настоящото становище няма да бъдат разгледани всички възможни сценарии. Технологиите, свързани с моделите на ИИ, са обект на бързо развитие; съответно съображенията на ЕКЗД в настоящото становище следва да се тълкуват в тази светлина.
17. **В настоящото становище не се анализират посочените по-долу разпоредби, които все пак може да играят важна роля при оценката на изискванията за защита на данните, приложими за моделите на ИИ:**
- **Обработване на специални категории данни:** ЕКЗД припомня забраната по член 9, параграф 1 от ОРЗД по отношение на обработването на специални категории данни и ограничените изключения по член 9, параграф 2 от ОРЗД¹¹. В това отношение Съдът на Европейския съюз („Съдът на ЕС“) допълнително пояснява, че *„когато съвкупност от данни, която включва едновременно чувствителни и нечувствителни данни, е предмет на такива операции, и по-специално се събира като цяло, без данните да могат да бъдат отделени едни от други към момента на това събиране, обработването на тази съвкупност от данни трябва да се счита за забранено по смисъла на член 9, параграф 1 от ОРЗД, щом съдържа поне една чувствителна данна и не е приложимо нито едно от изключенията, упоменати в член 9, параграф 2 от Регламента“*¹². Освен това Съдът на ЕС също така подчертава, че *„за целите на прилагането на изключението, предвидено в член 9, параграф 2, буква д) от ОРЗД, е нужно да се провери дали субектът на данни е възнамерявал изрично и чрез ясно потвърждаващо действие да направи въпросните лични данни достояние за широката общественост“*¹³. Тези съображения следва да се вземат предвид, когато обработването на лични данни в рамките на моделите на ИИ включва специални категории данни.

¹¹ Вж. също Доклада на ЕКЗД за работата, извършена от работната група за ChatGPT, приет на 23 май 2024 г., параграф 18: „По отношение на обработването на специални категории лични данни едно от изключенията на член 9, параграф 2 трябва да бъде приложимо в допълнение, за да бъде обработването законосъобразно. По принцип едно от тези изключения може да бъде член 9, параграф 2, буква д) от ОРЗД. Самият факт, че личните данни са публично достъпни, обаче не означава, че „субектът на данните явно е направил тези данни публично достояние“ [...]“.

¹² Решение на Съда на ЕС от 4 юли 2023 г., C-252/21, дело *Meta/Bundeskartellamt* (ECLI:EU:C:2023:537), точка 89.

¹³ Решение на Съда на ЕС от 4 юли 2023 г., дело C-252/21, *Meta/Bundeskartellamt* (ECLI:EU:C:2023:537), точка 77.

- **Автоматизирано вземане на решения, включително профилиране:** Операциите по обработване, извършвани в рамките на моделите на ИИ, може да попаднат в обхвата на член 22 от ОРЗД, по силата на който се налагат допълнителни задължения на администраторите и се предоставят допълнителни гаранции на субектите на данни. Във връзка с това ЕКЗД припомня своите Насоки относно автоматизираното вземане на индивидуални решения и профилирането за целите на Регламент (ЕС) 2016/679¹⁴.
- **Съвместимост на целите:** В член 6, параграф 4 от ОРЗД за определени правни основания са предвидени критерии, които администраторът трябва да вземе предвид с цел да установи дали обработването за друга цел е съвместимо с целта, за която първоначално са събрани личните данни. Тази разпоредба може да е от значение при разработването и внедряването на модели на ИИ и нейната приложимост следва да бъде оценена от НО.
- **Оценки на въздействието върху защитата на данните („ОВЗД“)** (член 35 от ОРЗД): ОВЗД са важен елемент от отчетността, когато обработването в рамките на моделите на ИИ е вероятно да доведе до висок риск за правата и свободите на физическите лица¹⁵.
- **Принцип на защита на данните при проектирането** (член 25, параграф 1 от ОРЗД): Защитата на данните при проектирането е съществена предпазна мярка, която трябва да бъде оценена от компетентните органи при разработването и внедряването на модел на ИИ.

2.2 Основни понятия

18. Като предварителна забележка ЕКЗД желае да предостави разяснения относно терминологията и концепциите, които използва в настоящото становище и само за целите на настоящото становище:
- **„Данни от първа ръка“** се отнася до личните данни, които администраторът е събрал от субектите на данни.
 - **„Данни от трети страни“** се отнася до лични данни, които администраторите не са получили от субектите на данни, а са събрали или получили от трета страна, например от брокер на данни, или чрез извличане на данни от интернет.
 - **„Извличането на данни от интернет“** е често използвана техника за събиране на информация от публично достъпни онлайн източници. Информацията, събрана например от услуги като новинарски медии, социални медии, дискусии във форуми и лични уебсайтове, може да съдържа лични данни.
 - Искането се отнася до **„жизнения цикъл“ на моделите на ИИ**, както и до различни етапи, отнасящи се, наред с другото, до „създаването“, „разработването“, „обучението“, „актуализирането“, „настройването“ или „последващото обучение“ на моделите на ИИ. ЕКЗД признава, че в зависимост от обстоятелствата такива етапи може да се провеждат при

¹⁴ Насоки на Работната група по член 29 („РГ29“) относно автоматизираното вземане на индивидуални решения и профилирането за целите на Регламент 2016/679, последно преразгледани и приети на 6 февруари 2018 г., одобрени от ЕКЗД на 25 май 2018 г. Вж. също Решение на Съда на ЕС от 7 декември 2023 г., дело C-634/21, *SCHUFA Holding и други* (ECLI:EU:C:2023:957).

¹⁵ Работна група 29, Насоки относно оценката на въздействието върху защитата на данни (ОВЗД) и определяне дали съществува вероятност обработването „да породи висок риск“ за целите на Регламент 2016/679, преразгледани и приети на 4 октомври 2017 г., одобрени от ЕКЗД на 25 май 2018 г.

разработването и внедряването на модели на ИИ и може да включват обработване на лични данни за различни цели на обработване. Въпреки това, за целите на настоящото становище ЕКЗД счита, че е важно да се рационализира категоризацията на етапите, които е вероятно да възникнат. Поради това за целите на настоящото становище ЕКЗД се позовава на „**етапа на разработване**“ и на „**етапа на внедряване**“. Разработването на модел на ИИ обхваща всички етапи преди всяко внедряване на модела на ИИ и включва, наред с другото, разработване на кодове, събиране на лични обучителни данни, предварително обработване на лични обучителни данни и обучение. Внедряването на модел на ИИ обхваща всички етапи, свързани с използването на модел на ИИ, и може да включва всички операции, извършвани след етапа на разработване. ЕКЗД е наясно с разнообразието от случаи на употреба и с потенциалните последици от тях за обработването на лични данни; поради това компетентните органи следва да преценят дали наблюденията, предоставени в настоящото становище, са от значение за обработването, което оценяват.

- ЕКЗД също така подчертава, че при необходимост терминът „**обучение**“ се отнася до частта от етапа на разработване, в която моделите на ИИ се учат от данните, за да изпълнят предвидената за тях задача (както е обяснено в следващия раздел на настоящото становище).
- Понятието и обхватът на **моделите на ИИ**, както се разбира от ЕКЗД за целите на настоящото становище, са допълнително уточнени в следващия специален раздел.

2.3 Моделите на ИИ в рамките на становището

19. В Акта на ЕС за изкуствения интелект („**Акт за ИИ**“)¹⁶ „система с ИИ“ се определя като „машинно базирана система, която е проектирана да работи с различни нива на автономност и която може да прояви адаптивност след внедряването си, и която, с явна или подразбираща се цел, въз основа на въведените в нея входящи данни, извежда начина на генериране на резултати като прогнози, съдържание, препоръки или решения, които могат да окажат влияние върху физическа или виртуална среда“¹⁷. В съображение 12 от Акт за ИИ допълнително е разяснено понятието „система с ИИ“. Съответно, ключова характеристика на системите с ИИ е тяхната способност да правят изводи. Техниките, които дават възможност за правене на изводи при изграждането на система с ИИ, включват машинно обучение, логически и основани на знания подходи.
20. От друга страна, „моделите на ИИ“ са само косвено установени в Акта за ИИ: *„Въпреки че моделите на ИИ са основни компоненти на системите с ИИ, сами по себе си те не представляват системи с ИИ. Моделите на ИИ налагат добавянето на допълнителни компоненти, като например потребителски интерфейс, за да се превърнат в системи с ИИ. Моделите на ИИ обикновено са интегрирани в системите с ИИ и са част от тях.“*¹⁸.
21. ЕКЗД разбира, че определението за модел на ИИ, предложено в искането, е по-тясно от определението в Акта за ИИ, тъй като с него „модел на ИИ“ се определя като *„обхващащ продукта, който произлиза от механизмите за обучение, прилагани към набор от*

¹⁶ Регламент (ЕС) 2024/1689 на Европейския парламент и на Съвета от 13 юни 2024 г. за установяване на хармонизирани правила относно изкуствения интелект и за изменение на регламенти (ЕО) № 300/2008, (ЕС) № 167/2013, (ЕС) № 168/2013, (ЕС) 2018/858, (ЕС) 2018/1139 и (ЕС) 2019/2144 и директиви 2014/90/ЕС, (ЕС) 2016/797 и (ЕС) 2020/1828 (Акт за изкуствения интелект).

¹⁷ Вж. член 3, параграф 1 от Акта за ИИ.

¹⁸ Съображение 97 от Акта за изкуствения интелект.

обучителни данни, в контекста с изкуствения интелект, машинното обучение, задълбоченото машинно учене или друг свързан контекст на обработване“ и допълнително се уточнява, че „Терминът се прилага за модели на ИИ, които е предвидено да преминат допълнително обучение, настройване и/или развитие, както и за модели на ИИ, за които това не е предвидено“.¹⁹

22. Въз основа на това ЕКЗД прие настоящото становище, като приема, че дадена система с ИИ ще разчита на модел на ИИ, за да изпълни предвидената цел, като включи модела в по-широка рамка (напр. система с ИИ за обслужване на клиенти може да използва модел на ИИ, обучен чрез исторически данни от разговори, за да предостави отговори на запитвания на потребители).
23. Освен това моделите на ИИ (или „**моделите**“), които са от значение за настоящото становище, са тези, които са разработени чрез процес на обучение. Този процес на обучение е част от етапа на разработване, при който моделите се учат от данните, за да изпълнят планираната си задача. Поради това за процеса на обучение е необходим набор от данни, от които моделът ще идентифицира и „учи“ модели. В тези случаи моделът ще използва различни техники, за да си изгради представа за знанията, извлечени от набора от данни от обучението. Такъв е по-специално случаят с машинното самообучение.
24. На практика всеки модел на ИИ е алгоритъм, чието функциониране се определя от набор от елементи. Например моделите на задълбочено машинно обучение често са под формата на невронна мрежа с множество слоеве, състоящи се от възли, свързани с ъгли с тежести, които се коригират по време на обучението, за да се научат връзките между входните и изходните данни. Характеристиките на един обикновен модел на задълбочено машинно обучение ще бъдат: i) вида и размера на всеки слой, ii) тежестта, придавана на всеки ъгъл (понякога наричан „параметри“), iii) функциите за активиране²⁰ между слоевете и евентуално iv) други операции, които може да се извършват между слоевете. Когато например се провежда обучение по обикновен модел на задълбочено машинно обучение за класификация на изображения, входните данни („**пиксели на изображенията**“) ще бъдат свързани с изходните данни и тежестите може да бъдат коригирани, така че в повечето случаи да се получат правилните изходни данни.
25. Други примери за модели за задълбочено машинно обучение включват ГЕМ и генеративен ИИ, които се използват например за генериране на съдържание, подобно на това, създадено от човека, и за създаване на нови данни.
26. **Въз основа на горните съображения и в съответствие с искането обхватът на настоящото становище обхваща само подгрупата от модели на ИИ, които са резултат от обучение на такива модели с лични данни.**

3 По съществото на искането

3.1 По съществото на моделите на ИИ във връзка с определението за лични данни

¹⁹ Искане, стр. 3.

²⁰ Т.е. функции, с които се изчисляват, въз основа на входните данни и тежестите, изходните данни на невронен възел, които след това ще бъдат изпратени до следващия слой на невралната мрежа.

27. В член 4, параграф 1 от ОРЗД личните данни се определят като *„всяка информация, свързана с идентифицирано физическо лице или физическо лице, което може да бъде идентифицирано“* (т.е. субекта на данните). Освен това в съображение 26 от ОРЗД се предвижда, че принципите за защита на данните не следва да се прилагат за анонимна информация, а именно информация, която не е свързана с идентифицирано физическо лице или физическо лице, което може да бъде идентифицирано, като се вземат предвид *„всички средства, за които има достатъчна вероятност да бъдат използвани“* от администратора или от друго лице. Това включва: i) данни, които никога не са били свързани с идентифицирано лице или лице, което може да бъде идентифициран; и ii) лични данни, които са анонимизирани по такъв начин, че субектът на данните не е или вече не може да бъде идентифициран.
28. Съответно на въпрос 1²¹ от искането може да се отговори, като се анализира дали модел на ИИ, получен в резултат на обучение, което включва обработване на лични данни, следва във всички случаи да се счита за анонимен. Въз основа на формулировката на въпроса в настоящия раздел ЕКЗД ще се позовава на процеса на „обучение“ на модел на ИИ.
29. На първо място ЕКЗД би желал да представи следните общи съображения. Моделите на ИИ, независимо дали са обучени с лични данни или не, обикновено са проектирани да правят прогнози или заключения, т.е. да правят изводи. Освен това моделите на ИИ, обучени с лични данни, често са проектирани да правят изводи за физически лица, различни от тези, чиито лични данни са били използвани за обучение на модела. Някои модели на ИИ обаче са специално проектирани да предоставят лични данни относно физически лица, чиито лични данни са били използвани за обучение или по някакъв начин за предоставяне на такива данни. В тези случаи, такива модели на ИИ по своята същност (и обикновено по необходимост) ще включват информация, свързана с идентифицирано физическо лице или физическо лице, което може да бъде идентифицирано, и поради това ще включват обработване на лични данни. Ето защо тези видове модели на ИИ не могат да се считат за анонимни. Такъв би бил например случаят i) на генеративен модел, настроен въз основа на гласовите записи на дадено лице, за да имитира неговия глас; или ii) всеки модел, проектиран да отговаря с лични данни от обучението, когато се изисква информация за конкретно лице.
30. Въз основа на горните съображения, в отговора на въпрос 1 от искането ЕКЗД акцентира върху ситуацията с моделите на ИИ, които не са проектирани да предоставят лични данни, свързани с обучителните данни.
31. ЕКЗД счита, че дори когато даден модел на ИИ не е бил умишлено проектиран да произвежда информация, свързана с идентифицирано физическо лице или физическо лице, което може да бъде идентифицирано, от обучителните данни, информацията от набора от обучителни данни, включително лични данни, все пак може да остане „абсорбирана“ в параметрите на модела, а именно представена чрез математически обекти. Те може да се различават от оригиналните обучителни данни, но все пак може да запазват оригиналната информация за тези данни, която в крайна сметка може да бъде извлечена или получена от модела по друг начин, пряко или косвено. Когато информация, свързана с идентифицирани лица или лица, които може да бъдат идентифицирани, чиито лични данни са използвани за обучение на модела, може да бъде получена от модел на ИИ със средства, за които може да се очаква, че е вероятно да бъдат използвани, може да се заключи, че този модел не е анонимен.

²¹ „Счита ли се, че окончателният модел на ИИ, който е бил обучен с помощта на лични данни, във всички случаи не отговаря на определението за лични данни (както е посочено в член 4, параграф 1 от ОРЗД)?“

32. Във връзка с това в искането се посочва, че „В съществуващите научни публикации се изтъкват някои потенциални уязвими страни, които могат да съществуват в моделите на ИИ и които могат да доведат до обработване на лични данни,²² както и до това обработването на лични данни да се извършва, когато моделите се внедряват за използване с други данни или чрез приложно-програмни интерфейси („API“), или чрез „бързи“ интерфейси“²³.
33. В същия дух научните изследвания в областта на извличането на обучителни данни са особено динамични²⁴. Това показва, че в някои случаи е възможно да се използват средства, за които е разумно вероятно да се извлекат лични данни от някои модели на ИИ, или просто да се получат случайно лични данни чрез взаимодействия с модел на ИИ (например като част от система с ИИ). Непрекъснатите научноизследователски усилия в тази област ще спомогнат за допълнително оценяване на остатъчните рискове от връщането²⁵ и извличането на лични данни във всеки отделен случай.
34. Въз основа на горепосочените съображения ЕКЗД счита, че моделите на ИИ, обучени чрез лични данни, не могат във всички случаи да се считат за анонимни. Вместо това преценката за това дали даден модел на ИИ е анонимен следва да се оценява въз основа на конкретни критерии за всеки отделен случай.

3.2 Относно обстоятелствата, при които моделите на ИИ биха могли да се считат за анонимни, и свързаните с тях доказателства

35. По отношение на въпрос 1 от искането²⁶ от ЕКЗД се изисква да изясни обстоятелствата, при които модел на ИИ, обучен с помощта на лични данни, може да се счита за анонимен. По отношение

²² Като например атаки с логически изводи за принадлежност ([OWASP](#)) и атаки чрез обръщане на модела ([OWASP](#) и [Veale et al](#), 2018 г.).

²³ Искане, стр. 1—2.

²⁴ Вж. в това отношение например: i) Veale M., Binns R., Edwards L., 2018 г., *Algorithms that remember: model inversion attacks and data protection law* (Алгоритми, които помнят: атаки чрез обръщане на модела и закон за защита на данните). Phil. Trans. R. Soc. A 376: 20180083, на разположение на <http://dx.doi.org/10.1098/rsta.2018.0083>; ii) Brown H., Lee K., Mireshghallah F., Shokri R., and Tramèr F., *What Does it Mean for a Language Model to Preserve Privacy?* (Какво означава един езиков модел да запазва поверителността?), 2022 г., ACM Digital Library, FAccT '22, 20 юни 2022 г., Сеул, Република Корея, на разположение на <https://dl.acm.org/doi/abs/10.1145/3531146.3534642>; iii) Vassilev A., Oprea A., Fordyce A., Anderson H., *Adversarial Machine Learning A Taxonomy and Terminology of Attacks and Mitigations* (Състезателно машинно обучение Таксономия и терминология на атаките и смекчаването им), януари 2024 г., National Institute of Standards and Technology, на разположение на <https://nvlpubs.nist.gov/nistpubs/ai/NIST.AI.100-2e2023.pdf>; iv) Carlini N., Tramèr F., Wallace E., Jagielski M., Herbert-Voss A., Lee K., Roberts A., Brown T., Song D., Erlingsson U., Oprea A., Raffel C., *Extracting Training Data from Large Language Models* (Извличане на данни за обучение от големи езикови модели), arXiv:2012.07805v2 [cs.CR] 15 юни 2021 г., на разположение на <https://arxiv.org/pdf/2012.07805>; v) Fredrikson M., Jha S., Ristenpart T., *Model Inversion Attacks that Exploit Confidence Information and Basic Countermeasures* (Атаки за обръщане на модела, които използват информация за доверието, и основни мерки за противодействие), ACM Digital Library, 12 октомври 2015 г., на разположение на <https://dl.acm.org/doi/abs/10.1145/2810103.2813677>; vi) Zhang Y., Jia R., Pei H., Wang W., Li B., Song D., *The Secret Revealer: Generative Model-Inversion Attacks Against Deep Neural Networks* (Разкривателят на тайните: Генеративни атаки с преобръщане на модела срещу дълбоки невронни мрежи), arXiv:1911.07135v2 [cs.LG] 18 април 2020 г., на разположение на <https://arxiv.org/pdf/1911.07135>.

²⁵ За система с ИИ, базирана на генеративен ИИ, връщането съответства на ситуацията, в която резултатите са пряко свързани с обучителните данни.

²⁶ „Какви са обстоятелствата, при които това може да се случи?“

на въпрос 1, точка i), буква а) от искането²⁷ от ЕКЗД се изисква да поясни кои доказателства и/или документация надзорните органи следва да вземат предвид, когато преценяват дали даден модел на ИИ е анонимен.

3.2.1 Общо съображение относно анонимизацията в разглеждания контекст

36. Използването на израза „всяка информация“ в определението за „лични данни“ в член 4, параграф 1 от ОРЗД отразява целта за определяне на широк обхват на това понятие, който да обхваща всички видове информация, при условие че тя „е свързана“ със субекта на данните, който е идентифициран или може да бъде идентифициран пряко или косвено.
37. Информацията може да се отнася до физическо лице дори когато е технически организирана или кодирана (например само в машинночетим формат, независимо дали е защитена или със свободен достъп) по начин, който не прави връзката с това физическо лице непосредствено очевидна. В такива случаи може да се използват софтуерни приложения за лесно идентифициране, разпознаване и извличане на специфични данни. Това важи в особена степен за моделите на ИИ, при които параметрите представляват статистически връзки между обучителните данни, и когато може да е възможно да се извлекат точни или неточни (защото са статистически изведени) лични данни пряко от връзките между данните, включени в модела, или чрез търсене в този модел.
38. Тъй като моделите на ИИ обикновено не съдържат записи, които може да бъдат директно изолирани или свързани, а по-скоро параметри, представляващи вероятностни връзки между данните, съдържащи се в модела, в реалистични сценарии може да е възможно да се изведе²⁸

²⁷ „В такъв случай как могат да бъдат доказани стъпките, които са били предприети, за да се гарантира, че моделът на ИИ не обработва лични данни?“

²⁸ (i) Carlini N., Chien S., Nasr M., Song S., Terzis A., Tramer F., *Membership Inference Attacks From First Principles* (Атаки с логически изводи за принадлежност от първите принципи), arXiv: 2112.03570, на разположение на <https://arxiv.org/abs/2112.03570>;

(ii) Crețu A.M., Guépin F., and De Montjoye Y.A, *Correlation inference attacks against machine learning models* (Атаки чрез корелационни логически изводи срещу модели за машинно обучение). Sci. Adv.10, eadj9260(2024). Doi:10.1126/sciadv.adj9260, на разположение на <https://www.science.org/doi/10.1126/sciadv.adj9260>;

(iii) Dana L., Pydi M. S., Chevalere Y., *Memorization in Attention-only Transformers* (Запаметяване в трансформатори, основани само на механизми за внимание) arXiv:2411.10115v1 [cs.AI] 15 ноември 2024 г., на разположение на: <https://arxiv.org/abs/2411.10115>;

(iv) Gehrke M., Liebenow J., Mohammadi E. & Braun T. et al. *Lifting in Support of Privacy-Preserving Probabilistic Inference* (Повдигане в подкрепа на вероятностен извод със запазване на поверителността). Künstl Intell, 13 юни 2024 г., на разположение на: <https://doi.org/10.1007/s13218-024-00851-y>;

(v) HU H., *Membership Inference Attacks and Defenses on Machine Learning Models Literature* (Атаки с логически изводи за принадлежност и защити във връзка с литература относно модели за машинно обучение), на разположение на: <https://github.com/HongshengHu/membership-inference-machine-learning-literature>;

(vi) Nasr M., Carlini N., Hayase J., Jagielski M., Cooper A. F., Ippolito D., Choquette-Choo C. A., Wallace E., Tramèr F., and Lee K., *Scalable Extraction of Training Data from (Production) Language Models* (Масшабно извличане на данни за обучение от (производствени) езикови модели), arXiv:2311.17035 28 ноември 2023 г., на разположение на: <https://arxiv.org/abs/2311.17035>;

(vii) Shokri R., Stronati M., Song C., Shmatikov V., *Membership Inference Attacks against Machine Learning Models* (Атаки с логически изводи за принадлежност срещу модели за машинно обучение) arXiv:1610.05820v2 [cs.CR], 31 март 2017 г., на разположение на <https://arxiv.org/abs/1610.05820>;

(viii) Staab R., Vero M., Mislav Balunović, Martin Vechev, 2024 г., *Beyond Memorization: Violating Privacy Via Inference with Large Language Models* (Отвъд запаметяването: Нарушаване на неприкосновеността на личния

информация от модела, като например извод за принадлежност. Следователно, за да може надзорният орган да се съгласи с администратора, че даден модел на ИИ може да се счита за анонимен, той следва да провери най-малко дали е получил достатъчно доказателство, че с разумни средства: i) личните данни, свързани с обучителните данни, не могат да бъдат ²⁹ извлечени от модела; и ii) никой от резултатите, получени при търсене в модела, не се отнася до субектите на данни, чиито лични данни са използвани за обучение на модела.

39. НО следва да вземат предвид три елемента при оценката на това дали тези условия са изпълнени.
40. Първо, НО следва да вземат предвид елементите, посочени в последните становища на Работната група по член 29 и/или насоките на ЕКЗД по този въпрос. По отношение на анонимизацията към датата на настоящото становище НО следва да вземат предвид елементите, включени в Становище 05/2014 на Работната група по член 29 относно техническите способности за анонимизиране (**„Становище 05/2014 на Работната група по член 29“**), в което се посочва, че ако не е възможно да изведе, свърже и извърши предположение за информация от предполагаемо анонимния набор от данни, данните може да се считат за анонимни³⁰. В него също така се посочва, че *„ако дадено предложение не отговаря на някой от критериите, следва да се извърши обстойна оценка на идентификационните рискове“*³¹. **Като се има предвид горепосочената вероятност за извличане и извършване на предположение, ЕКЗД счита, че е много вероятно моделите на ИИ да налагат такава задълбочена оценка на рисковете от идентифициране.**
41. Второ, тази оценка следва да бъде направена, като се вземат предвид *„всички средства, които биха могли да бъдат използвани разумно“* от администратора или друго лице за идентифициране на физически лица³², като определянето на тези средства следва да се основава на обективни фактори, както е обяснено в съображение 26 от ОРЗД, които може да включват:

живот чрез изводи с големи езикови модели), arXiv:2310.07298v2, 6 май 2024 г., на разположение на <https://arxiv.org/abs/2310.07298>;

(ix) Wu F., Cui L., Yao S., Yu S., *Inference Attacks in Machine Learning as a Service: A Taxonomy, Review, and Promising Directions* (Атаки с логически изводи при машинното обучение като услуга: Таксономия, преглед и обещаващи насоки) arXiv: 2406.02027v1 [cs.LG], 27 юни 2024 г., на разположение на <https://arxiv.org/abs/2406.02027v1>;

(x) Zhang J., Das D., Kamath G., Tramèr F., *Membership Inference Attacks Cannot Prove that a Model Was Trained On Your Data* (Атаките с логически изводи за принадлежност не могат да докажат, че модел е обучен чрез вашите данни) arXiv:2409.19798v1, [cs.LG], 29 септември 2024 г., на разположение на <https://arxiv.org/abs/2409.19798>;

(xi) Zhou Z., Xiang J., Chen C., and Su S., *Quantifying and Analyzing Entity-Level Memorization in Large Language Models* (Количествено определяне и анализ на запаметяването на ниво същностен обект в големи езикови модели), arXiv:2308.15727v2 [cs.CL] 5 ноември 2023 г., на разположение на: <https://arxiv.org/abs/2308.15727>.

²⁹ Извличането включва по-специално случая, в който личните данни се извличат от самия модел на ИИ, без или с малко използване на интерфейсите за търсене.

³⁰ Становище 05/2014 на Работната група по член 29, стр. 24.

³¹ Становище 05/2014 на Работната група по член 29, стр. 24.

³² Решение на Съда на ЕС от 19 октомври 2016 г., дело C-582/14, *Breyer/Bundesrepublik Deutschland* (ECLI:EU:C:2016:779), точка 43.

- a. характеристиките на самите обучителни данни, модела на изкуствения интелект и процедурата за обучение³³;
 - b. контекстът, в който моделът на ИИ се пуска и/или обработва³⁴;
 - c. допълнителната информация, която би позволила установяването на самоличността и може да бъде на разположение на даденото лице;
 - d. разходите и времето, от което лицето ще се нуждае, за да получи такава допълнителна информация (в случай че тя все още не е на негово разположение)³⁵; и
 - e. наличната технология към момента на обработването, както и технологичното развитие³⁶.
42. На трето място НО следва да преценят дали администраторите са оценили риска от идентифициране от страна на администратора и от различни видове „други лица“, включително от непредвидения достъп на трети страни до модела на ИИ, като също така се вземе предвид дали може основателно да се счита, че те могат да получат достъп или да обработват въпросните данни.
43. В обобщение ЕКЗД счита, че за да може даден модел на ИИ да се счита за анонимен, като се използват разумни средства, както i) вероятността за пряко (включително вероятно) извличане на лични данни по отношение на лицата, чиито лични данни са били използвани за обучението на модела; така и ii) вероятността за получаване, умишлено или не, на такива лични данни от запитвания, следва да бъдат незначителни³⁷ за всеки субект на данни. По подразбиране надзорните органи следва да имат предвид, че моделите на ИИ вероятно ще налагат задълбочена оценка на вероятността от идентифициране, за да се стигне до заключение относно възможния им анонимен характер. Тази вероятност следва да бъде оценена, като се вземат предвид *всички средства, които биха могли да бъдат използвани разумно* от администратора или друго лице, както и възможността за непреднамереното (повторно) използване или разкриване на модела.

3.2.2 Елементи за оценка на остатъчната вероятност за идентифициране

44. Въпреки че могат да бъдат предприети мерки както на етапа на разработване, така и на етапа на внедряване, за да се намали вероятността модел на ИИ да получи лични данни, при оценката на анонимността на модела следва също така да се вземе предвид прекият достъп до него.
45. Освен това надзорните органи трябва да оценяват за всеки отделен случай дали мерките, въведени от администратора, за да гарантира и докаже, че даден модел на ИИ е анонимен, са подходящи и ефективни.

³³ Това включва характеристики като уникалност на записите в обучителните данните, прецизност на информацията, агрегиране, рандомизация, и по-специално как те влияят върху уязвимостта към идентификация.

³⁴ Това включва контекстуални елементи, като например ограничаване на достъпа само до някои лица и правни гаранции.

³⁵ Решение на Съда на ЕС от 7 март 2024 г., дело C-479/22 P, *ОС/Европейска комисия* (ECLI:EU:C:2024:215), точка 50.

³⁶ Решение на Съда на ЕС от 7 март 2024 г., дело C-479/22 P, *ОС/Европейска комисия* (ECLI:EU:C:2024:215), точка 50.

³⁷ Решение на Съда на ЕС от 19 октомври 2016 г., дело C-582/14, *Breyer/Bundesrepublik Deutschland* (ECLI:EU:C:2016:779), точка 46, и Решение на Съда на ЕС от 7 март 2024 г., дело C-479/22 P, *ОС/Европейска комисия* (ECLI:EU:C:2024:215), точка 51.

46. По-специално, заключението от оценката на НО може да се различава между общодостъпен модел на ИИ, който е наличен за неизвестен брой хора с неизвестен набор от методи за изпитване и извличане на лични данни, и вътрешен модел на ИИ, достъпен само за служителите. Макар че и в двата случая НО следва да проверят дали администраторите са изпълнили задължението си за отчетност съгласно член 5, параграф 2 и член 24 от ОРЗД, „средствата, които биха могли да бъдат използвани разумно от други лица“, може да окажат въздействие върху обхвата и естеството на възможните сценарии, които трябва да бъдат разгледани. Поради това, в зависимост от контекста на разработването и внедряването на модела, надзорните органи може да обмислят различни нива на изпитване и устойчивост на атаки.
47. В това отношение ЕКЗД представя по-долу незадължителен и неизчерпателен списък на възможните елементи, които надзорните органи може да вземат предвид при оценката на твърдението на администратора за анонимност. Възможно е да има и други подходи, ако те предлагат еквивалентно ниво на защита, по-специално, като се вземе предвид съвременното технологично равнище.
48. Наличието или отсъствието на изброените по-долу елементи не е решаващ критерий за оценка на анонимността на даден модел на ИИ.

3.2.2.1 Проектиране на модел на ИИ

49. Що се отнася до проектирането на модела на ИИ, компетентните органи следва да оценят подходите, използвани от администраторите по време на етапа на разработване. В това отношение следва да се разгледа прилагането и ефективността на четири ключови области (посочени по-долу).

Избор на източници

50. Първата област на оценка включва проверка на подбора на източниците, използвани за обучение на модела на ИИ. Това включва оценка от страна на надзорните органи на всички стъпки, предприети за избягване или ограничаване на събирането на лични данни, включително, наред с другото, i) целесъобразността на критериите за избор; ii) целесъобразността и адекватността на избраните източници, като се има(т) предвид предвидената(ите) цел(и); и iii) дали са изключени неподходящи източници.

Подготовка и свеждане до минимум на данните

51. Втората област на оценка е свързана с подготовката на данни за етапа на обучение. НО следва да проучат по-специално: i) дали е било обмислено използването на анонимни и/или лични данни, които са преминали псевдонимизация; и ii) когато е било решено да не се използват такива мерки, причините за това решение, като се вземе предвид предвидената цел; iii) стратегиите и техниките за свеждане до минимум на данните, използвани за ограничаване на обема на личните данни, включени в процеса на обучение; и iv) всички процеси на филтриране на данни, прилагани преди обучението по модел, предназначени за премахване на лични данни, които не са от значение.

Методологически решения по отношение на обучението

52. Третата област на оценка е свързана с избора на надеждни методи при разработването на модели на ИИ. НО следва да оценяват методологическите избори, които може значително да намалят или премахнат възможността за идентификация, включително, наред с другото: i) дали при тази методология се използват методи за регулиране, за да се подобри обобщаването на модела и да се намали прекомерното приспособяване; и, най-важното, ii) дали администраторът е приложил подходящи и ефективни техники за запазване на неприкосновеността на личния живот (напр. диференциална неприкосновеност).

Мерки по отношение на изходните данни от модела

53. Последната област на оценка се отнася до всички методи или мерки, добавени към самия модел на ИИ, които може да не окажат въздействие върху риска от пряко извличане на лични данни за модела от всеки, имащ пряк достъп до него, но които могат да намалят вероятността от получаване на лични данни, свързани с обучителни данни от заявки.

3.2.2.2 Анализ на модела на ИИ

54. Първата стъпка, която трябва да предприемат НО, за да оценят надеждността на проектирания модел на ИИ по отношение на анонимизацията, е да се уверят, че проектът е разработен по план и подлежи на ефективно инженерно управление. НО следва да оценят дали администраторите са извършили одити, основани на документи (вътрешни или външни), които включват оценка на избраните мерки и на тяхното въздействие, за да се ограничи вероятността за идентифициране. Това би могло да включва анализ на докладите от прегледи на кодове, както и теоретичен анализ, при който се документира целесъобразността на избраните мерки за намаляване на вероятността от повторно идентифициране при съответния модел.

3.2.2.3 Изпитване на модели на ИИ и устойчивост на атаки

55. И накрая, НО следва да вземат предвид обхвата, честотата, количеството и качеството на изпитванията, които администраторът е провел за модела. По-специално, НО следва да вземат предвид, че успешното изпитване, което обхваща широкоизвестни атаки и такива на съвременно технологично равнище, може да бъде само доказателство за устойчивостта на тези атаки. Към датата на настоящото становище това би могло да включва, наред с другото, структурирани изпитвания спрямо: i) извод за вменяване на отговорност и за принадлежност; ii) изтичане; iii) връщане на данни за обучение; iv) обръщане на модела; или v) атаки за реконструкция.

3.2.2.4 Документация

56. Съгласно членове 5, 24, 25 и 30 от ОРЗД, а в случаите на вероятно висок риск за правата и свободите на субектите на данни — член 35 от ОРЗД, от администраторите се изисква да документират по подходящ начин своите операции по обработване. Това се отнася и за всяко обработване, което включва обучение на модел на ИИ, дори ако целта на обработването е анонимизиране. НО следва да вземат предвид тази документация и всяка редовна оценка на произтичащите рискове за обработването, извършвано от администраторите, тъй като те са основни стъпки за доказването, че не се обработват лични данни.
57. **ЕКЗД счита, че НО следва да вземат предвид документацията винаги когато трябва да се оцени искане за анонимност във връзка с даден модел на ИИ. ЕКЗД отбелязва, че ако НО не е в състояние да потвърди след оценка на твърдението за анонимност, включително с оглед на документацията, че са предприети ефективни мерки за анонимизиране на модела на ИИ, НО ще бъде в позиция да счита, че администраторът не е изпълнил задълженията си за отчетност съгласно член 5, параграф 2 от ОРЗД. Поради това следва да се разгледа и съответствието с други разпоредби на ОРЗД.**
58. В идеалния случай надзорните органи следва да проверят дали документацията на администратора включва:
- всякаква информация, свързана с ОВЗД, включително всички оценки и решения, с които се определя, че не е необходимо да се извършва ОВЗД;
 - всички съвети или обратна информация, предоставени от длъжностното лице по защита на данните („ДЛЗД“) (когато ДЛЗД е било или е трябвало да бъде назначено);

- c. информация за техническите и организационните мерки, предприети при проектирането на модела на ИИ, за да се намали вероятността от идентифициране, включително модела на заплахата и оценките на риска, на които се основават тези мерки. Това следва да включва конкретните мерки за всеки източник на набори от обучителни данни, включително съответните URL адреси на източници и описания на предприятиите (или вече предприети от доставчици на набори от данни — трети страни) мерки;
- d. техническите и организационните мерки, предприети на всички етапи през целия жизнен цикъл на модела, които или са допринесли за липсата на лични данни в модела, или са я потвърдили;
- e. документацията, доказваща теоретичната устойчивост на модела на ИИ към техники за повторна идентификация, както и проверките, предназначени за ограничаване или оценяване на успеха и въздействието на основните атаки (връщане, атаки за логически извод за принадлежност, изтичане и др.). Това може да включва по-специално: (i) съотношението между количеството обучителни данни и броя на параметрите в модела, включително анализ на въздействието му върху модела³⁸; (ii) показатели за вероятността за повторна идентификация въз основа на съвременното технологично равнище; (iii) доклади за това как е бил тестван моделът (от кого, кога, как и в каква степен) и (iv) резултатите от тестовете;
- f. документацията, предоставена на администратора(ите), който(ито) използва(т) модела, и/или на субектите на данни, по-специално документацията, свързана с мерките, предприети за намаляване на вероятността за идентифициране и по отношение на възможните остатъчни рискове.

3.3 Относно целесъобразността на легитимния интерес като правно основание за обработване на лични данни в контекста на разработването и внедряването на модели на ИИ

59. За да отговори на въпроси 2 и 3 от искането, ЕКЗД първо ще представи общи наблюдения относно някои важни аспекти, които компетентните органи следва да вземат предвид, независимо от правното основание за обработване, когато оценяват как администраторите може да докажат спазването на ОРЗД в контекста на моделите на ИИ. След това ЕКЗД, въз основа на Насоки 1/2024 относно обработването на лични данни въз основа на член 6, параграф 1, буква е) от ОРЗД³⁹, ще вземе под внимание трите стъпки, изисквани от оценката на легитимния интерес в контекста на разработването и внедряването на модели на ИИ.

³⁸ Ricciato F., *A Cautionary Reflection on (Pseudo-)Synthetic Data from Deep Learning on Personal Data (Внимателен преглед относно (псевдо)синтетичните данни от задълбочено машинно обучение относно личните данни)*, конференция „Поверителност в статистическите бази данни“ (PSD 2024), Антиб, Франция, септември 2024 г., слайдове на разположение на: https://cros.ec.europa.eu/system/files/2024-10/20240926_PSD2024_Ricciato_v6_1.pdf и Belkin M., Hsu D., Ma S., & Mandal S. (2019 г.), *Reconciling modern machine-learning practice and the classical bias-variance tradeoff (Съгласуване на съвременната практика за машинно обучение и класическия модел на компромис между отклонение и вариация)*. Сборник на Националната академия на науките, 24 юли 2019 г., 116(32) 15849-15854, на разположение на: <https://www.pnas.org/doi/10.1073/pnas.1903070116>

³⁹ Вж. Насоки 1/2024 на ЕКЗД относно обработването на лични данни въз основа на член 6, параграф 1, буква е) от ОРЗД, версия 1.0, приети на 8 октомври 2024 г.

3.3.1 Общи коментари

60. ЕКЗД припомня, че в ОРЗД не е установена йерархия между различните правни основания, предвидени в член 6, параграф 1 от ОРЗД⁴⁰.
61. В член 5 от ОРЗД се определят принципите, свързани с обработването на лични данни. ЕКЗД подчертава тези, които са от значение за настоящото становище и следва най-малкото да бъдат взети под внимание от НО при оценката на конкретни модели на ИИ, както и най-значимите изисквания от други разпоредби на ОРЗД, като се има предвид обхватът на настоящото становище.
62. **Принцип на отчетност** (член 5, параграф 2 от ОРЗД) — Съгласно този принцип администраторът носи отговорност за спазването на ОРЗД и е в състояние да докаже това спазване. В тази връзка ролята и отговорностите на страните, които обработват лични данни в рамките на разработването или внедряването на модел на ИИ, трябва да бъдат оценени, преди да се извърши обработване, за да се определят задълженията на администраторите или съвместните администратори, както и на обработващите лични данни (ако има такива) от самото начало.
63. **Принципи на законосъобразност, добросъвестност и прозрачност** (член 5, параграф 1, буква а) от ОРЗД) — Когато се оценява законосъобразността на обработването в рамките на моделите на ИИ в светлината на член 6, параграф 1 от ОРЗД ЕКЗД счита, че е полезно да се прави разграничение между различните етапи на обработването на лични данни⁴¹. Принципът на справедливост, който е тясно свързан с принципа на прозрачност, налага личните данни да не се обработват чрез несправедливи методи или чрез измама, или по начин, който е *„неоправдано вреден, незаконосъобразно дискриминационен, неочакван или подвеждащ за субекта на данните“*⁴². Поради това, предвид сложността на използваните технологии, информацията за обработването на лични данни в рамките на моделите на ИИ следва да се предоставя по достъпен, разбираем и лесен за ползване начин⁴³. Прозрачността относно обработването на лични данни включва, по-специално, спазването на задълженията за предоставяне на информация, посочени в членове 12—14 от ОРЗД⁴⁴, според които също се изисква, в случай на автоматизирано вземане на решения, включително профилиране, значима информация относно използваната логика, както и значението и предвидените последствия от обработването за субекта на данните⁴⁵. Като се има предвид, че етапите на разработване на модели на ИИ може да включват събирането на големи количества данни от общодостъпни източници (като например чрез техники за извличане на данни от интернет), позоваването на изключението,

⁴⁰ Пак там, точка 1.

⁴¹ Доклад на ЕКЗД за работата, извършена от работната група за ChatGPT, приет на 23 май 2024 г., точка 14.

⁴² Доклад на ЕКЗД за работата, извършена от работната група за ChatGPT, приет на 23 май 2024 г., точка 23; Насоки 4/2019 на ЕКЗД относно член 25 относно защитата на данните на етапа на проектирането и по подразбиране, версия 2.0, приета на 20 октомври 2020 г., точка 69; член 29 Насоки на работната група относно прозрачността съгласно Регламент 2016/679, преразгледани и приети на 11 април 2018 г., одобрени от ЕКЗД на 25 май 2018 г., параграф 2.

⁴³ Насоки на работната група по член 29 относно прозрачността съгласно Регламент 2016/679, преразгледани и приети на 11 април 2018 г., одобрени от ЕКЗД на 25 май 2018 г., точка 5.

⁴⁴ Вж. също съображение 39 от ОРЗД, което гласи, че *„За физическите лица следва да е прозрачно по какъв начин отнасящи се до тях лични данни се събират, използват, консултират или обработват по друг начин, както и в какъв обхват се извършва или ще се извършва обработването на данните [...]“*.

⁴⁵ Член 13, параграф 2, буква е) от ОРЗД и член 14, параграф 2, буква ж) от ОРЗД.

предвидено в член 14, параграф 5, буква б) от ОРЗД, е строго ограничено до случаите, когато изискванията на тази разпоредба са изцяло изпълнени⁴⁶.

64. **Принципи за ограничение на целите и свеждане на данните до минимум** (член 5, параграф 1, букви б) и в) от ОРЗД) — В съответствие с принципа за свеждане на данните до минимум разработването и внедряването на модели на ИИ налага личните данни да бъдат подходящи, свързани със и необходими по отношение на целта. Това може да включва обработването на лични данни, за да се избегнат рисковете от потенциални пристрастия и грешки, когато това е ясно и конкретно определено в рамките на целта и личните данни са необходими за тази цел (напр. те не могат да бъдат ефективно постигнати чрез обработване на други данни, включително синтетични или анонимизирани данни)⁴⁷. Работна група 29 вече е подчертала, че *„целта на събирането трябва да бъде ясно и точно определена [...]“*⁴⁸. Когато се преценява дали преследваната цел е законна, конкретна и изрична и дали обработването е в съответствие с принципа за свеждане на данните до минимум, най-напред следва да се определи съответната дейност по обработване. По-специално, различните етапи в рамките на фази на разработване или внедряване може да представляват едни и същи или различни дейности по обработване и може да включват отделни или съвместни администратори. В някои случаи е възможно на ранен етап на развитие да се определи целта, която ще се преследва по време на внедряването на модела на ИИ. Дори когато случаят не е такъв, част от контекста за това внедряване вече следва да е ясен и следователно следва да се обмисли по какъв начин този контекст определя целта на разработването. Когато преразглеждат целта на обработването на даден етап от разработването, НО следва да очакват известна степен на детайлност от администратора(ите) и обяснение как тези детайли допринасят за целта на обработването. Това може да включва например информация за вида на разработения модел на ИИ, очакваните му функционалности и всякакъв друг приложим контекст, който вече е известен на този етап. Процесът на внедряване би могъл също да включва, например, дали даден модел се разработва за вътрешно внедряване, дали администраторът възнамерява да продаде или разпространява модела на трети страни след неговото разработване, включително дали моделът е предназначен предимно за научноизследователски или търговски цели.
65. **Права на субектите на данни** (глава III от ОРЗД) — Независимо от необходимостта надзорните органи да гарантират, че всички права на субекта на данни се спазват, когато администраторите разработват и внедряват модели на ИИ, ЕКЗД припомня, че когато администраторът се позовава на легитимен интерес като правно основание, правото на възражение съгласно член 21 от ОРЗД се прилага и следва да бъде гарантирано⁴⁹.

⁴⁶ Доклад на ЕКЗД за работата, извършена от работната група за ChatGPT, приет на 23 май 2024 г., точка 27.

⁴⁷ Освен това в член 10, параграф 5 от Акта за ИИ се предвиждат специални правила за обработването на специални категории лични данни във връзка с високорисковите системи с ИИ с цел да се гарантира откриване и коригиране на предубедеността.

⁴⁸ Становище 3/2013 на работната група по член 29 относно ограничението на целите (РД 203), страници 15—16.

⁴⁹ Съгласно член 21 от ОРЗД, ако субект на данни възрази на основания, свързани с неговото конкретно положение, срещу обработването на лични данни, които го засягат, администраторът прекратява обработването на личните данни, освен ако не докаже, че съществуват убедителни законови основания за обработването, които имат предимство пред интересите, правата и свободите на субекта на данни, или за установяването, упражняването или защитата на правни претенции. Следователно двата аспекта, които

3.3.2 Съображения относно трите стъпки на оценката на легитимния интерес при разработването и внедряването на модели на ИИ

66. За да определят дали дадено обработване на лични данни може да се основава на член 6, параграф 1, буква е) от ОРЗД, НО следва да проверят дали администраторите внимателно са оценили и документирали изпълнението на следните три кумулативни условия:
- i) преследването на легитимен интерес от страна на администратора или на трета страна;
 - ii) обработването е необходимо за преследването на легитимния интерес; и
 - iii) легитимният интерес не е затруднен от интересите или основните права и свободи на субектите на данни⁵⁰.

3.3.2.1 Първа стъпка — Преследване на легитимен интерес от страна на администратора или от трета страна

67. Интересът е по-широкият интерес или полза, която администраторът или третата страна може да има при извършването на конкретна дейност по обработване⁵¹. Въпреки че ОРЗД и Съдът на ЕС признават няколко интереса за легитимни⁵², оценката на легитимността на даден интерес следва да бъде резултат от анализ на всеки отделен случай.
68. Както припомня ЕКЗД в своите Насоки относно легитимния интерес⁵³, даден интерес може да се счита за легитимен, ако са изпълнени следните три кумулативни критерия:
- a. Интересът е законен⁵⁴;
 - b. Интересът е ясно и точно определен; и
 - c. Интересът е реален и актуален, а не спекулативен.

трябва да се вземат под внимание от НО, са дали администраторът е в състояние да докаже тези неопровержими имащи преимущество законни основания и дали правото на възражение може да бъде упражнено.

⁵⁰ Съд на ЕС, решение от 4 юли 2023 г., дело C-252/21, *Meta/Bundeskartellamt* (ECLI:EU:C:2023:537), точка 106; Съд на ЕС, решение от 11 декември 2019 г., дело C-708/18, *Asociația de Proprietari bloc M5A-Scara A* (ECLI:EU:C:2019:1064), точка 40. Вж. също Насоки 1/2024 на ЕКЗД относно обработването на лични данни въз основа на член 6, параграф 1, буква е) от ОРЗД, версия 1.0, приета на 8 октомври 2024 г., точка 12 и сл. Както се напомня в настоящите насоки, тази „оценка следва да бъде направена в началото на обработването, с участието на длъжностното лице по защита на данните (ДЛЗД) (ако е определено), и следва да бъде документирана от администратора в съответствие с принципа на отчетност, посочен в член 5, параграф 2 от ОРЗД“.

⁵¹ Насоки 1/2024 на ЕКЗД относно обработването на лични данни въз основа на член 6, параграф 1, буква е) от ОРЗД, версия 1.0, приети на 8 октомври 2024 г., точка 14.

⁵² Насоки 1/2024 на ЕКЗД относно обработването на лични данни въз основа на член 6, параграф 1, буква е) от ОРЗД, версия 1.0, приети на 8 октомври 2024 г., точка 16.

⁵³ Насоки 1/2024 на ЕКЗД относно обработването на лични данни въз основа на член 6, параграф 1, буква е) от ОРЗД, версия 1.0, приети на 8 октомври 2024 г., точка 17.

⁵⁴ Решение на Съда на ЕС от 4 октомври 2024 г., дело C-621/22, *Koninklijke Nederlandse Lawn Tennisbond* (ECLI:EU:C:2024:857), точка 49, където Съдът на ЕС подчертава, че легитимен интерес не може да противоречи на закона. В това отношение ЕКЗД подчертава, че в зависимост от случая законодателните рамки следва да се вземат под внимание при оценяване на законосъобразността на даден интерес. Вж. например: Член 26, параграф 3 и член 28 от Регламент (ЕС) 2022/2065 на Европейския парламент и на Съвета от 19 октомври 2022 г. относно единния пазар на цифрови услуги и за изменение на Директива 2000/31/ЕО (Акт за цифровите услуги) („ЗИД на ЗП“) относно забранената целева реклама за малолетни и непълнолетни; член 5, параграфи 1 и 2 от Акта за ИИ относно забранените практики в областта на ИИ (манипулативни практики и практики под прага на осъзнаване); обработване в нарушение на правата на интелектуална собственост и разпоредбите на Директива (ЕС) 2019/790 относно авторското право и сродните му права в цифровия единен пазар.

69. В зависимост от другите две стъпки, изисквани от оценката на легитимния интерес, следните примери може да представляват легитимен интерес в рамките на моделите на ИИ: i) разработване на услугата на агент за разговор в помощ на потребителите; ii) разработване на система с ИИ за откриване на измамно съдържание или поведение; и iii) подобряване на откриването на заплахи в информационна система.

3.3.2.2 Втора стъпка — Анализ на необходимостта от обработването за преследване на легитимния интерес

70. Втората стъпка от оценката се състои в това да се определи дали обработването на лични данни е необходимо за целите на преследвания легитимен интерес (интереси)⁵⁵ („критерий за необходимост“).
71. В съображение 39 от ОРЗД се пояснява, че *„личните данни следва да се обработват, единствено ако целта на обработването не може да бъде постигната в достатъчна степен с други средства“*. Според Съда на ЕС и предишните насоки на ЕКЗД условието, свързано с необходимостта от обработването, следва да се разглежда в светлината на основните права и свободи на субектите на данни и във връзка с принципа за свеждане на данните до минимум, заложен в член 5, параграф 1, буква в) от ОРЗД⁵⁶.
72. В методологията, посочена от Съда на ЕС, се взема предвид контекстът на обработването, както и последиците за администратора и за субектите на данни. Следователно, оценката на необходимостта включва два елемента: i) дали дейността по обработване ще даде възможност преследването на целта⁵⁷; и ii) дали няма по-малко инвазивен начин за постигане на тази цел⁵⁸.

⁵⁵ Насоки 1/2024 на ЕКЗД относно обработването на лични данни въз основа на член 6, параграф 1, буква е) от ОРЗД, версия 1.0, приети на 8 октомври 2024 г., точки 28—30.

⁵⁶ Решение на Съда на ЕС от 4 юли 2023 г., дело C-252/21, *Meta/Bundeskartellamt* (ECLI:EU:C:2023:537), точки 108 и 109, като се прави позоваване и на Решение на СЕС от 11 декември 2019 г., дело C-708/18, *Asociația de Proprietari bloc M5A-ScaraA* (ECLI:EU:C:2019:1064), точка 48; Решение на Съда на ЕС от 9 ноември 2010 г., съединени дела C-92/09 и C-93/09, *Volker und Markus Schecke* (ECLI:EU:C:2010:662), точки 85 и 86; Съд на ЕС, решение от 22 юни 2021 г., дело C-439/19, *Latvijas Republikas Saeima* (ECLI:EU:C:2021:504), точки 98, 109, 110 и 113. Вж. също например: Насоки на ЕКЗД 3/2019 относно обработването на лични данни чрез видеоустройства, версия 2.0, приети на 29 януари 2020 г., точки 24—26 и 73; Насоки на ЕКЗД 2/2019 относно обработването на лични данни съгласно член 6, параграф 1, буква б) от ОРЗД при предоставянето на онлайн услуги на субектите на данни, версия 2.0, приети на 8 октомври 2019 г., точки 23—25; Становище на ЕКЗД 11/2024 относно използването на лицево разпознаване за рационализиране на пътничеството на летищата, версия 1.1, прието на 23 май 2024 г., точка 27.

⁵⁷ Вж. решение на Съда на ЕС от 16 декември 2008 г., дело C-524/06, *Heinz Huber срещу Bundesrepublik Deutschland* (ECLI:EU:C:2008:724), точка 66. Също така по същото дело, вж. заключението на генералния адвокат Poiares Maduro по дело C-524/06, *Heinz Huber срещу Bundesrepublik Deutschland* (ECLI:EU:C:2008:194), точка 16, в което се посочва: *„подходящият критерий в случая е ефективността и националната юрисдикция следва да го приложи. Въпросът, който тя трябва да постави, е дали има други начини за обработване на данни, чрез които имиграционните власти да приложат нормите относно статута на пребиваване. Ако националната юрисдикция даде положителен отговор на този въпрос, централизираното съхранение и обработване на данни на гражданите на Съюза следва да бъде обявено за неправомерно. Не е необходимо алтернативната система да бъде най-ефективната или най-подходящата; достатъчно е да функционира адекватно. С други думи, дори ако централният регистър е по-ефективен или по-удобен, или по-лесен за ползване от алтернативите му (например децентрализираните, местни регистри), очевидно последните са за предпочитане, ако в тях има данни за статута на пребиваване на гражданите на Съюза“*.

⁵⁸ Вж. решение на Съда на ЕС от 27 септември 2017 г., дело C-73/16, *Peter Puškár* (ECLI:EU:C:2017:725), точка 113: *„Така, от компетентността на запитващата юрисдикция е да провери дали съставянето*

73. Например, и в зависимост от случая, предвиденият обем лични данни, включени в модела на ИИ, трябва да бъде оценен с оглед на по-малко инвазивни алтернативи, за които разумно може да се очаква да бъдат налични, за да се постигне също толкова ефективно целта на преследвания легитимен интерес. Ако преследването на целта е възможно и чрез модел на ИИ, който не включва обработване на лични данни, то обработването на лични данни следва да не се счита за необходимо. Това е особено важно за разработването на модели на ИИ. Когато преценяват дали е изпълнено условието за необходимост, компетентните органи следва да обърнат специално внимание на обема на обработваните лични данни и дали той е пропорционален на преследването на въпросния легитимен интерес, също и с оглед на принципа за свеждане на данните до минимум.
74. При оценката на необходимостта следва също така да се вземе предвид по-широкият контекст на планираното обработване на лични данни. Съществуването на средства, които са по-щадящи по отношение на основните права и свободи на субектите на данни, може да варира в зависимост от това дали администраторът има пряка връзка със субектите на данни (данни от първа ръка) или не (данни от трети страни). Съдът на ЕС предостави някои съображения, които трябва да се вземат предвид при анализа на необходимостта от обработване на данни от първа ръка за целите на преследвания(те) легитимен(ни) интерес(и) (макар и в контекста на разкриването на такива данни от трети страни)⁵⁹.
75. Прилагането на технически гаранции за защита на личните данни също може да допринесе за спазване на критерия за необходимост. Това би могло да включва например мерки за прилагане като посочените в раздел 3.2.2 по такъв начин, че да не се постига анонимизиране, но с което все пак се намалява лекотата, с която субектите на данни могат да бъдат идентифицирани. ЕКЗД отбелязва, че някои от тези мерки, когато не се изискват за спазване на ОРЗД, може да представляват допълнителни предпазни мерки, както е анализирано допълнително в подраздела „Смекчаващи мерки“ в рамките на раздел 3.3.2.3⁶⁰.

3.3.2.3 Трета стъпка — сравнителен тест

76. Третата стъпка от оценката на легитимния интерес е **„сравнение“** (наричано в настоящия документ също **„сравнителен тест“**)⁶¹. Тази стъпка се състои в определяне и описване на различните засегнати противоположни права и интереси⁶², т.е., от една страна интересите, основните права и свободи на субектите на данни, а от друга страна — интересите на администратора или на трета страна. В такъв случай следва да се счита, че конкретните

на спорния списък и включването в него на имената на заинтересованите лица са подходящи за осъществяване на преследваните с това съставяне цели и дали не са налице други по-малко ограничителни способности за постигането на тези цели“; Вж. също например Заключение на генералния адвокат Rantos по дело C-252/21, *Meta/Bundeskartellamt*, ECLI:EU:C:2022:704, точка 61, в което се посочва: „[...] Следователно, при липсата на алтернативи, които в по-голяма степен зачитат защитата на личните данни, е необходимо да е налице тясна връзка между обработването и преследвания интерес, защото не е достатъчно обработването да е просто от полза за администратора“.

⁵⁹ Съд на ЕС, решение от 4 октомври 2024 г., дело C-621/22, *Koninklijke Nederlandse Lawn Tennisbond* (ECLI:EU:C:2024:857), точки 51—53.

⁶⁰ Вж. Насоки 1/2024 на ЕКЗД относно обработването на лични данни въз основа на член 6, параграф 1, буква е) от ОРЗД, версия 1.0, приети на 8 октомври 2024 г., точка 57.

⁶¹ Вж. Насоки 1/2024 на ЕКЗД относно обработването на лични данни въз основа на член 6, параграф 1, буква е) от ОРЗД, версия 1.0, приети на 8 октомври 2024 г., точки 31—60.

⁶² Вж. Насоки 1/2024 на ЕКЗД относно обработването на лични данни въз основа на член 6, параграф 1, буква е) от ОРЗД, версия 1.0, приети на 8 октомври 2024 г., точка 32.

обстоятелства по случая доказват, че легитимният интерес е подходящо правно основание за въпросните дейности по обработване⁶³.

Интереси, основни права и свободи на субектите на данни

77. В член 6, параграф 1, буква е) от ОРЗД е предвидено, че при оценката на различните компоненти в рамките на сравнителния тест администраторът следва да вземе предвид интересите, основните права и свободите на субектите на данни. Интересите на субектите на данни са тези, които може да бъдат засегнати от въпросното обработване. При етапа на разработване на модел на ИИ те може да включват, но не се ограничават до интереса за самостоятелно определяне и запазване на контрола върху собствените лични данни (например данните, събрани за разработването на модела). При внедряването на модел на ИИ интересите на субектите на данни може да включват, но без да се ограничават до интереси за запазване на контрола върху собствените лични данни (напр. данните, обработвани след внедряването на модела), финансови интереси (напр. когато даден модел на ИИ се използва от субекта на данни за генериране на приходи или се използва от физическо лице в рамките на неговата професионална дейност), лични ползи (напр. когато даден модел на ИИ се използва за подобряване на достъпността до определени услуги) или социално-икономически интереси (напр. когато даден модел на ИИ дава възможност за достъп до по-добро здравеопазване или улеснява упражняването на основно право, като например достъп до образование)⁶⁴.
78. Колкото по-точно даден интерес е определен с оглед на предвидената цел на обработването, толкова по-голяма възможност ще дава за ясно отчитане на реалността на ползите и рисковете, които трябва да се вземат предвид при сравнителния тест.
79. По отношение на основните права и свободи на субектите на данни разработването и внедряването на модели на ИИ може да породят сериозни рискове за правата, защитени от Хартата на основните права на ЕС („Хартата на ЕС“), включително, но не само правото на личен и семеен живот (член 7 от Хартата на ЕС) и правото на защита на личните данни (член 8 от Хартата на ЕС). Тези рискове може да възникнат по време на етапа на разработване, например, когато личните данни се извличат против желанията на субектите на данни или без тяхно знание. Тези рискове може да възникнат и на етапа на внедряване, например когато личните данни се обработват от модела (или като част от него) по начин, който противоречи на правата на субектите на данни, или когато е възможно да се направи извод, случайно или чрез атаки (напр. извод за принадлежност, извличане или обръщане на модела), за това какви лични данни се съдържат в базата от обучителни данни. Такива ситуации представляват риск за неприкосновеността на личния живот на субектите на данни, чиито данни могат да се появят на етапа на внедряване на системата с ИИ (напр. риск за репутацията, кражба на самоличност или измама, риск за сигурността в зависимост от естеството на данните).
80. В зависимост от разглеждания случай може да има и рискове за други основни права. Широкомасштабното и безразборно събиране на данни от модели на ИИ на етапа на разработване например може да създаде усещане за наблюдение у субектите на данни, особено като се имат предвид трудностите за предотвратяване на събирането на публични данни. Това може да подтикне хората към автоцензура и да породят рискове от подкопаване на свободата им на

⁶³ Вж. Насоки 1/2024 на ЕКЗД относно обработването на лични данни въз основа на член 6, параграф 1, буква е) от ОРЗД, версия 1.0, приети на 8 октомври 2024 г., точка 32, в които се прави позоваване и на решение на Съда на ЕС от 4 юли 2023 г., дело C-252/21, *Meta срещу Bundeskartellamt* (ECLI:EU:C:2023:537), точка 110.

⁶⁴ Вж. Насоки 1/2024 на ЕКЗД относно обработването на лични данни въз основа на член 6, параграф 1, буква е) от ОРЗД, версия 1.0, приети на 8 октомври 2024 г., точка 38.

изразяване (член 11 от Хартата на ЕС). На етапа на внедряване съществуват и рискове за свободата на изразяване, когато моделите на ИИ се използват за блокиране на публикуването на съдържание от субектите на данни. Освен това модел на ИИ, който препоръчва неподходящо съдържание на уязвими лица, може да представлява риск за тяхното психично здраве (член 3, параграф 1 от Хартата на ЕС). В други случаи внедряването на модели на ИИ може да доведе и до неблагоприятни последици за правото на лицето на труд (член 15 от Хартата на ЕС), например когато кандидатурите за работа се подбират предварително с помощта на модел на ИИ. По същия начин моделът на ИИ би могъл да представлява риск за правото на недискриминация (член 21 от Хартата на ЕС), ако дискриминира физическите лица въз основа на определени лични характеристики (като националност или пол). Освен това внедряването на модели на ИИ може също така да представлява риск за сигурността и безопасността на отделните лица (напр. когато моделът на ИИ се използва злонамерено), както и рискове за тяхната физическа и психическа неприкосновеност⁶⁵.

81. Внедряването на модели на ИИ може също така да окаже положително въздействие върху някои основни права, напр. моделът може да подкрепя правото на психическа неприкосновеност на лицето (член 3 от Хартата), например когато модел на ИИ се използва за откриване на вредно съдържание онлайн; или моделът може да улесни достъпа до определени основни услуги или да улесни упражняването на основните права, като например достъпа до информация (член 11 от Хартата на ЕС) или достъпа до образование (член 14 от Хартата на ЕС).

Въздействие на обработването върху субектите на данните

82. Обработването на лични данни, което се извършва по време на етапите на разработване и внедряване на модели на ИИ, може да окаже въздействие върху субектите на данни по различни начини, които могат да бъдат положителни или отрицателни⁶⁶. Ако например дадена дейност по обработване води до ползи за субекта на данните, тези ползи може да се вземат под внимание при сравнителния тест. Макар че наличието на такива ползи може да доведе до заключение на НО, че интересите на администратора или на трета страна нямат преимущество пред интересите, основните права и свободи на субектите на данни, това заключение може да бъде резултат само от анализ на отделния случай, при който се вземат предвид всички подходящи фактори.
83. Въздействието на обработването върху субектите на данни може да се повлияе от i) естеството на данните, обработвани от моделите, ii) контекста на обработването и iii) допълнителните последици, които обработването може да има⁶⁷.
84. Във връзка с **естеството на обработваните данни** следва да се припомни, че освен специалните категории лични данни и данните, свързани с присъди и нарушения, които се ползват съответно с допълнителна защита съгласно членове 9 и 10 от ОРЗД, обработването на някои други категории лични данни може да доведе до значителни последици за субектите на данни. В този смисъл за обработването на определени видове лични данни, които разкриват изключително поверителна информация (напр. финансови данни или данни за местонахождение) с цел разработването и внедряването на модел на ИИ, следва да се счита, че е възможно да има сериозно въздействие върху субектите на данни. На етапа на внедряване последиците от такова

⁶⁵ Насоки 1/2024 относно обработването на лични данни въз основа на член 6, параграф 1, буква е) от ОРЗД, версия 1.0, приети на 8 октомври 2024 г., точка 46.

⁶⁶ Вж. Насоки 1/2024 на ЕКЗД относно обработването на лични данни въз основа на член 6, параграф 1, буква е) от ОРЗД, версия 1.0, приети на 8 октомври 2024 г., точка 39.

⁶⁷ Вж. Насоки 1/2024 на ЕКЗД относно обработването на лични данни въз основа на член 6, параграф 1, буква е) от ОРЗД, версия 1.0, приети на 8 октомври 2024 г., точка 32.

обработване за физическите лица може да бъдат например икономически (напр. дискриминация в контекста на заетостта) и/или репутационни (напр. клеветата).

85. Във връзка с **контекста на обработването** е необходимо първо да се определят елементите, които биха могли да създадат рискове за субектите на данни (например начинът, по който е разработен моделът, начинът, по който моделът може да бъде внедрен, и/или дали мерките за сигурност, използвани за защита на личните данни, са подходящи). Характерът на модела и предвиденото оперативно използване изпълняват ключова роля при определянето на такива потенциални причини.
86. Необходимо е също така да се оцени сериозността на тези рискове за субектите на данни. Може да се вземе предвид, наред с другото, по какъв начин се обработват личните данни (напр. дали се комбинират с други набори от данни), какъв е мащабът на обработването и обемът на обработваните лични данни⁶⁸ (напр. общият обем на данните, обемът на данните за всеки субект на данни, броят на засегнатите субекти на данни)⁶⁹, статутът на субекта на данни (напр. деца или други уязвими субекти на данни) и връзката му с администратора (напр. ако субектът на данни е клиент). Например използването на извличане на данни от интернет на етапа на разработване може да доведе — при липса на достатъчни предпазни мерки — до значително въздействие върху физическите лица поради големия обем на събраните данни, големия брой субекти на данни и безразборното събиране на лични данни.
87. **Допълнителните последици**, които обработването може да има, следва да се вземат предвид и при оценката на въздействието на обработването върху субектите на данни. Те следва да се оценяват от надзорните органи за всеки отделен случай, като се вземат предвид конкретните факти, които се разглеждат.
88. Такива последици може да включват (но без да се ограничават до) рискове от нарушаване на основните права на субектите на данни, както е описано в предходния подраздел⁷⁰. Рисковете може да варират по вероятност и сериозност и да произтичат от обработване на лични данни, което може да доведе до физически, материални или нематериални вреди, по-специално, когато обработването може да доведе до дискриминация⁷¹.
89. Когато внедряването на модел на ИИ предполага обработване на лични данни както на i) субектите на данни, чиито лични данни са включени в набора от данни, използван на етапа на разработване, така и на ii) физически лица, чиито лични данни се обработват на етапа на внедряване, НО следва да разграничават и вземат предвид рисковете, засягащи интересите, правата и свободите на всяка от тези категории субекти на данни, когато проверяват сравнителния тест, проведен от администратора.
90. **И накрая, при анализа на възможните допълнителни последици от обработването следва да се вземе предвид и вероятността от настъпването на тези допълнителни последици.** Оценката на тази вероятност следва да се извършва, като се вземат предвид действащите технически и организационни мерки и специфичните обстоятелства по случая. НО например може да

⁶⁸ Вж. Насоки 1/2024 на ЕКЗД относно обработването на лични данни въз основа на член 6, параграф 1, буква е) от ОРЗД, версия 1.0, приети на 8 октомври 2024 г., точка 43.

⁶⁹ Решение на Съда ЕС от 4 юли 2023 г., дело C-252/21, *Meta.Bundeskartellamt* (ECLI:EU:C:2023:537), точка 116.

⁷⁰ Вж. подраздел „Интереси, основни права и свободи на субектите на данни“ по-горе.

⁷¹ Вж. раздел 2.3 от Насоки 1/2024 на ЕКЗД относно обработването на лични данни въз основа на член 6, параграф 1, буква е) от ОРЗД, версия 1.0, приети на 8 октомври 2024 г. Вж. също съображение 75 от ОРЗД за допълнителни примери.

преценят дали са приложени мерки за избягване на потенциална злоупотреба с модела на ИИ. За модели на ИИ, които може да бъдат внедрени за различни цели, като например генеративен ИИ, това може да включва проверки, които ограничават във възможно най-голяма степен използването на моделите за вредни практики, например: създаването на убедителни фалшификати; чатботове, които се използват за дезинформация, фишинг и други видове измами; и манипулативни ИИ/агенти с ИИ (по-специално когато те са антропоморфни или предоставят подвеждаща информация).

Разумни очаквания на субектите на данни

91. Въз основа на съображение 47 от ОРЗД, „[в]ри всички случаи, за установяването на законен интерес би била необходима внимателна преценка, включително дали субектът на данни може по времето и в контекста на събирането на данни основателно да очаква, че може да се осъществи обработване на личните данни за тази цел. Интересите и основните права на субекта на данни биха могли по-конкретно да имат преимущество пред интереса на администратора, когато личните данни се обработват при обстоятелства, при които субектите на данни основателно не очакват по-нататъшна обработка“⁷².
92. Разумните очаквания изпълняват ключова роля в сравнителния тест, не на последно място поради сложността на използваната в моделите на ИИ технология и факта, че за субектите на данни може да е трудно да разберат разнообразието от потенциални употреби на даден модел на ИИ и съответното обработване на данни⁷³. За тази цел може да се вземе предвид предоставената информация на физическите лица, за да се прецени дали субектите на данни могат основателно да очакват, че техните лични данни ще бъдат обработвани. Въпреки че пропускането на информация може да допринесе до това лицата да не очакват определено обработване, изпълнението на изискванията за прозрачност, посочени в ОРЗД, само по себе си не е достатъчно, за да се счита, че субектите на данни могат разумно да очакват дадено обработване⁷⁴. Освен това само защото информацията, свързана с етапа на разработване на даден модел на ИИ, е включена в политиката за поверителност на администратора, това не означава непременно, че субектите на данни могат разумно да очакват това да се случи, а по-скоро това следва да бъде анализирано от НО въз основа на конкретните обстоятелства по случая и като се вземат предвид всички съответни фактори.
93. Когато се оценяват разумните очаквания на субектите на данни във връзка с обработването, което се извършва на етапа на разработването, е важно да се направят справки с елементите, посочени в Насоките на ЕКЗД относно легитимния интерес⁷⁵. Освен това в рамките на предмета на настоящото становище е важно да се вземе предвид по-широкият обхват на обработването.

⁷² Вж. също Решение на Съда на ЕС от 4 юли 2023 г., дело C-252/21, *Meta/Bundeskartellamt* (ECLI:EU:C:2023:537), точка 112; СЕС, решение от 11 декември 2019 г., дело C-708/18, *Asociația de Proprietari bloc M5A-Scara A* (ECLI:EU:C:2019:1064), точка 58; Решение на Съда на ЕС от 4 октомври 2024 г., C-621/22, *Koninklijke Nederlandse Lawn Tennisbond* (ECLI:EU:C:2024:857), точка 55.

⁷³ В решение от 4 юли 2023 г. по дело C-252/21, *Meta/Bundeskartellamt* (ECLI:EU:C:2023:537), точка 123, например, въпреки че Съдът на ЕС е установил, че „подобряване на продукта“ по принцип не може да бъде изключено като легитимен интерес, той е установил също, че „изглежда съмнително [...] дали целта за подобряване на продукта може — предвид обхвата на това обработване и значителните му последици за ползвателя, както и факта, че няма основание последният да очаква тези данни да бъдат обработени [...] — да има преимущество пред интересите и основните права на такъв ползвател, още повече когато ползвателят е дете“.

⁷⁴ Насоки 1/2024 относно обработването на лични данни въз основа на член 6, параграф 1, буква е) от ОРЗД, версия 1.0, приети на 8 октомври 2024 г., точка 53.

⁷⁵ Насоки 1/2024 относно обработването на лични данни въз основа на член 6, параграф 1, буква е) от ОРЗД, версия 1.0, приети на 8 октомври 2024 г., точки 50—54.

Това може да включва, макар и да не се ограничава до това дали личните данни са били публично достъпни или не, естеството на отношенията между субекта на данните и администратора (и дали съществува връзка между тях), естеството на услугата, целта, за която са събрани личните данни, източника, от който са събрани данните (напр. уебсайта или услугата, където са събрани личните данни, и настройките за поверителност, които те предлагат), потенциалното по-нататъшно използване на модела и дали физическите лица всъщност знаят, че личните им данни са онлайн.

94. На етапа на разработване на модела разумните очаквания на субектите на данни може да се различават в зависимост от това дали данните, обработвани за разработването на модела, се оповестяват публично от субектите на данни или не. Освен това разумните очаквания може да се различават и в зависимост от това дали те са предоставили данните директно на администратора (напр. в рамките на използването на услугата), или администраторът ги е получил от друг източник (напр. чрез трета страна или извличане на данни от интернет). И в двата случая стъпките, предприети за информиране на субектите на данни за дейностите по обработване, следва да се вземат предвид при оценката на разумните очаквания.
95. На етапа на внедряване на модела на ИИ е също толкова важно да се вземат предвид разумните очаквания на субектите на данни в рамките на специфичните способности на модела. За моделите на ИИ, които могат да се адаптират в зависимост от предоставените данни, може например да е подходящо да се разгледа дали субектите на данни са знаели, че са предоставили лични данни, за да може моделът на ИИ да адаптира отговорите си към техните нужди и за да могат те да получат персонализирани услуги. Освен това може да е подходящо да се прецени дали тази дейност по обработване ще окаже въздействие само върху услугата, предоставяна на субектите на данни (напр. персонализирането на съдържание за конкретен потребител), или дали тя ще се използва за промяна на услугата, предоставяна на всички клиенти (напр. за подобряване на модела по общ начин). Както на етапа на разработване, може също така да е особено подходящо да се прецени дали съществува пряка връзка между субектите на данни и администратора. Такава пряка връзка може например да позволява на администратора лесно да предоставя информация на физическите лица относно дейността по обработване и модела, което след това би могло да повлияе върху разумните очаквания на тези лица.

Смекчаващи мерки

96. Когато интересите, правата и свободите на субектите на данни изглежда надделяват над легитимните интереси на администратора или на трета страна, администраторът може да обмисли въвеждането на смекчаващи мерки за ограничаване на въздействието на обработването върху тези субекти на данни. Смекчаващите мерки са предпазни мерки, които следва да бъдат съобразени с обстоятелствата по случая и зависят от различни фактори, включително от планираното използване на модела на ИИ. Тези мерки за смекчаване на риска имат за цел да гарантират, че интересите на администратора или на трета страна няма да бъдат обезсилени, така че администраторът да може да се позовава на това правно основание.
97. Както се припомня в Насоките на ЕКЗД относно легитимния интерес, смекчаващите мерки не следва да се бъркат с мерките, които администраторът е длъжен да приеме по закон така или иначе, за да гарантира спазването на ОРЗД, независимо дали обработването се основава на

член 6, параграф 1, буква е) от ОРЗД⁷⁶. Това е особено важно за мерките, които например налагат спазване на принципите на ОРЗД, като принципа за свеждане на данните до минимум.

98. Списъкът с мерки, предоставен по-долу, не е изчерпателен и не съдържа предписания, и прилагането на мерките следва да се разглежда въз основа на оценка на всеки отделен случай. Въпреки че в зависимост от обстоятелствата някои от мерките по-долу може да бъдат необходими за спазване на специфичните задължения по ОРЗД, когато това не е така, те може да се вземат под внимание като допълнителни гаранции. Освен това някои от посочените по-долу мерки се отнасят до области, които са обект на бързо и ново развитие, и следва да се вземат под внимание от НО при разглеждането на конкретния случай.
99. **Във връзка с етапа на разработване на моделите на ИИ** може да се предприемат няколко мерки за намаляване на рисковете, породени от обработването на данни както от първа ръка, така и от трети страни (включително за намаляване на рисковете, свързани с практиките за извличане на данни от интернет). Въз основа на гореизложеното ЕКЗД предоставя някои примери за мерки, които може да се приложат за смекчаване на рисковете, установени при сравнителния тест, и следва да се вземат предвид от надзорните органи при оценката на конкретни модели на ИИ за всеки отделен случай.
100. **Технически мерки:**
- а. Мерки, посочени в раздел 3.2.2, които са подходящи за намаляване на съществуващите рискове, когато тези мерки не водят до анонимизиране на модела и не се изискват за спазване на други задължения по ОРЗД или съгласно критерия за необходимост (втората стъпка от оценката на легитимния интерес).
101. В допълнение към тях други подходящи мерки може да включват:
- б. Мерки за псевдонимизация: това може например да включва мерки за предотвратяване на каквото и да е комбиниране на данни въз основа на индивидуални идентификатори. Тези мерки може да не са подходящи, когато НО счита, че администраторът е доказал разумната необходимост от събиране на различни данни за конкретно физическо лице за разработването на въпросната система с ИИ или модел на ИИ.
 - с. Мерки за прикриване на лични данни или замяната им с фалшиви лични данни в учебния набор (напр. замяна на имена и адреси на електронна поща с фалшиви имена и фалшиви адреси на електронна поща). Тази мярка може да бъде особено подходяща, когато действителното съдържание на данните по същество не е от значение за цялостното обработване (например в обучението на ГЕМ).
102. **Мерки, които улесняват упражняването на правата на физическите лица:**
- а. Спазване на разумен период между събирането на набор от обучителни данни и неговото използване. Тази допълнителна гаранция може да позволи на субектите на данни да упражняват правата си през този период, като разумният период се оценява в зависимост от обстоятелствата във всеки отделен случай.
 - б. Предлагање на безусловен „отказ“ от самото начало, например чрез предоставяне на субектите на данни на право да възразят по собствена преценка преди извършването

⁷⁶ Насоки 1/2024 относно обработването на лични данни въз основа на член 6, параграф 1, буква е) от ОРЗД, версия 1.0, приети на 8 октомври 2024 г., точка 57.

на обработването, за да се засили контролът на физическите лица върху техните данни, което надхвърля условията на член 21 от ОРЗД⁷⁷.

- c. Позволяване на субектите на данни да упражняват правото си на изтриване, дори когато конкретните основания, изброени в член 17, параграф 1 от ОРЗД, не се прилагат⁷⁸.
- d. Предоставяне на възможност на субектите на данни да подават искания за връщане или запамятаване на лични данни, както и обстоятелствата и средствата, чрез които исканията могат да бъдат възпроизведени, с което да се даде възможност на администраторите да възпроизведат и оценят съответните техники за отучване с цел да разглеждат исканията.

103. **Мерки за прозрачност:** в някои случаи смекчаващите мерки биха могли да включват мерки, които осигуряват по-голяма прозрачност по отношение на разработването на модела на ИИ. Някои мерки, в допълнение към спазването на задълженията по ОРЗД, може да спомогнат за преодоляване на информационната асиметрия и да позволят на субектите на данни да разберат по-добре обработването, което се извършва на етапа на разработване:

- a. Публикуване на публични и леснодостъпни съобщения, които не са ограничени до информацията, изисквана съгласно член 13 или 14 от ОРЗД, например чрез предоставяне на допълнителна информация относно критериите за събиране и всички използвани набори от данни, като се взема предвид специалната защита на децата и уязвимите лица.
- b. Алтернативни форми за информиране на субектите на данни, например: медийни кампании с различни медии за информиране на субектите на данни, информационна кампания по електронна поща, използване на графична визуализация, често задавани въпроси, етикети за прозрачност и карти с модели, чието систематизиране би могло да даде структура на представянето на информация за моделите на ИИ, и годишни доклади за прозрачност на доброволна основа.

104. **Специфични смекчаващи мерки в контекста на извличането на данни от интернет:** Като се има предвид, че както е посочено по-горе, извличането на данни от интернет създава специфични рискове⁷⁹, в този смисъл могат да бъдат определени конкретни мерки за намаляване на риска. Когато е уместно, те могат да се вземат предвид от надзорните органи в допълнение към посочените по-горе смекчаващи мерки, при проверяване на администратори, които извършват извличане на данни от интернет.

105. Специфичните мерки, когато не са необходими съгласно втората стъпка от оценката на легитимния интерес, може да се окажат полезни за намаляване на риска при извличането на данни от интернет. Те може да включват **технически мерки**, като например:

- a. Изключване на данни от публикации, които могат да включват лични данни, криещо рискове за определени лица или групи лица (напр. лица, които могат да бъдат обект на

⁷⁷ Пак там.

⁷⁸ Пак там.

⁷⁹ Тези практики може да повдигнат и допълнителни въпроси, които не са разгледани в настоящото становище, вж. например Pagallo U., Ciani Sciolla J., *Anatomy of web data scraping: ethics, standards, and the troubles of the law* (Анатомия на извличането на данни от интернет: етика, стандарти и проблеми със закона). *European Journal of Privacy Law & Technologies* (Европейски вестник за правото и технологиите в областта на неприкосновеността на личния живот), (2023 г.) 2 стр. 1—19, на разположение на: <https://doi.org/10.57230/EJPLT232PS>.

злоупотреби, щети или дори физически вреди, ако информацията бъде оповестена публично).

- b. Гарантиране, че определени категории данни не се събират или че определени източници са изключени от събирането на данни; това би могло да включва например някои уебсайтове, които са особено инвазивни поради чувствителния характер на предмета им.
- c. Изключване на събирането на данни от уебсайтове (или части от уебсайтове), които ясно се противопоставят на извличането на данни от интернет и повторното използване на тяхното съдържание за целите на създаването на бази данни за обучение на ИИ (например чрез зачитане на файловете robots.txt или ai.txt или друг признат механизъм за заявяване на изключване от автоматизирано обхождане или извличане на данни от интернет).
- d. Налагане на други подходящи ограничения на събирането, евентуално включващи критерии, основани на периоди.

106. В рамките на извличането на данни от интернет примери за конкретни мерки, **които улесняват упражняването на правата на физическите лица и прозрачността**, може да включват: създаване на списък за отказ, управляван от администратора и позволяващ на субектите на данни да възразят срещу събирането на техните данни на определени уебсайтове или онлайн платформи, като предоставят информация, която ги идентифицира на тези уебсайтове, включително преди събирането на данни⁸⁰.

107. **Специфични съображения по отношение на смекчаващите мерки на етапа на внедряване:** Въпреки че някои от посочените по-горе мерки също може да бъдат от значение и за етапа на внедряване, в зависимост от обстоятелствата ЕКЗД представя по-долу неизчерпателен списък на допълнителни мерки за подпомагане, които може да бъдат приложени и които следва да бъдат оценявани от НО за всеки отделен случай.

- a. Може например да бъдат въведени **технически мерки** за предотвратяване на съхранението, връщането или генерирането на лични данни, особено в рамките на генеративни модели на ИИ (като филтри за изходни данни), и/или за намаляване на риска от незаконна повторна употреба от модели на ИИ с общо предназначение (напр. цифров воден знак на резултатите, генерирани от ИИ).
- b. **Мерки, които улесняват или ускоряват упражняването на правата на физическите лица** на етапа на внедряване, отвъд това, което се изисква от закона, по-специално и не само по отношение на упражняването на правото на изтриване на лични данни от изходящи данни на модела или премахване на дублирането, както и техники след обучението, които имат за цел премахването или ограничаването на лични данни.

108. Когато разследват внедряването на конкретен модел на ИИ, проверяващите органи следва да проверят дали администраторът е публикувал проведения от него сравнителен тест, тъй като това може да увеличи прозрачността и справедливостта. Както е посочено в Насоките на ЕКЗД относно легитимния интерес, може да се обмислят други мерки за предоставяне на субектите на

⁸⁰ Освен ако администраторът докаже, че съществуват убедителни законови основания за обработването, които имат предимство пред интересите, правата и свободите на субекта на данни, или за установяването, упражняването или защитата на правни претенции.

данни на информация от сравнителния тест преди каквото и да е събиране на лични данни⁸¹. Освен това ЕКЗД подчертава⁸², че елемент, който трябва да се вземе под внимание, е дали администраторът е ангажирал длъжностното лице по защита на данните, когато е приложимо.

3.4 Относно възможното въздействие на незаконосъобразното обработване при разработването на модел на ИИ върху законосъобразността на последващото обработване или експлоатация на модела на ИИ

109. В настоящия раздел от становището се разглежда въпрос 4 от искането. Този въпрос има за цел да се разясни възможното въздействие на незаконосъобразното обработване на етапа на разработване върху последващото обработване (например на етапа на внедряване на модела на ИИ) или върху функционирането на модела. Въпросът има за цел да се разгледа както ситуацията, в която такъв модел на ИИ обработва лични данни, които се запазват в модела (въпрос 4, буква и) от искането), така и ситуацията, в която във внедряването на модела на ИИ вече не се извършва обработване на лични данни (т.е. моделът е анонимен) (въпрос 4, подточка ii) от искането).
110. Преди да разгледа някои конкретни сценарии, ЕКЗД представя следните общи съображения.
111. Първо, предоставените в настоящия раздел пояснения ще бъдат съсредоточени върху обработването на лични данни по време на етапа на разработване, извършвано при неспазване на принципа за законосъобразност, определен в член 5, параграф 1, буква а) от ОРЗД, и по-специално в член 6 от ОРЗД (наричан по-нататък „незаконосъобразност“)⁸³. В същия дух съображенията на ЕКЗД ще акцентират върху въздействието на неправомерността на обработването на етапа на разработване върху законосъобразността (т.е. спазването на член 5, параграф 1, буква а) от ОРЗД и член 6 от ОРЗД) на последващото обработване или функциониране на модела. ЕКЗД обаче посочва, че обработването, извършено на етапа на разработване, може да доведе и до нарушения на други разпоредби на ОРЗД, като липса на прозрачност по отношение на субектите на данни или защита на данните на етапа на проектиране и/или по подразбиране, които нарушения не са анализирани в настоящото становище.
112. Второ, при разглеждането на този въпрос принципът на отчетност, според който администраторите трябва да носят отговорност и да доказват спазването, *inter alia*, на член 5, параграф 1 от ОРЗД и член 6 от ОРЗД⁸⁴, играе ключова роля. Това важи и за необходимостта да се прецени коя организация е администратор на въпросната дейност по обработване и дали възникват ситуации на съвместно администриране (тъй като те може да бъдат неразривно свързани)⁸⁵. Като се има предвид значението на фактическите обстоятелства по всеки случай, включително по отношение на ролята на всяка страна, участваща в обработването,

⁸¹ Насоки 1/2024 на ЕКЗД относно обработването на лични данни въз основа на член 6, параграф 1, буква е) от ОРЗД, версия 1.0, приети на 8 октомври 2024 г., точка 68.

⁸² Насоки 1/2024 на ЕКЗД относно обработването на лични данни въз основа на член 6, параграф 1, буква е) от ОРЗД, версия 1.0, приети на 8 октомври 2024 г., точка 12.

⁸³ Съд на ЕС, решение от 4 май 2023 г., дело C-60/22, *Bundesrepublik Deutschland* (ECLI:EU:C:2023:373), точки 55—57.

⁸⁴ Съд на ЕС, решение от 4 май 2023 г., дело C-60/22, *Bundesrepublik Deutschland* (ECLI:EU:C:2023:373), точка 53.

⁸⁵ Насоки на ЕКЗД 7/2020 относно понятията „администратор“ и „обработващ лични данни“ в ОРЗД, версия 2.1, приети на 7 юли 2021 г., точка 55.

съображенията на ЕКЗД следва да се разбират като общи наблюдения, които надзорните органи трябва да оценяват за всеки отделен случай.

113. На трето място, ЕКЗД подчертава, че в съответствие с член 51, параграф 1 от ОРЗД компетентните органи са *„отговорни за наблюдението на прилагането на [ОРЗД], за да се защитят основните права и свободи на физическите лица във връзка с обработването и да се улесни свободното движение на личните данни в рамките на Съюза („надзорен орган“)“*. Поради това надзорните органи имат компетентността да оценяват законосъобразността на обработването и да упражняват правомощията си, предоставени по линия на ОРЗД, в съответствие с националната си рамка⁸⁶. В такива случаи надзорните органи разполагат с дискреционни правомощия да оценяват възможното(ите) нарушение(я) и да избират подходящи, необходими и пропорционални мерки измежду посочените в член 58 от ОРЗД, като вземат предвид обстоятелствата във всеки отделен случай⁸⁷.
114. **Когато е установено нарушение, НО, вземайки предвид обстоятелствата във всеки отделен случай, може да наложат корективни мерки, като например да разпоредят на администраторите да предприемат действия за отстраняване на незаконосъобразността на първоначалното обработване.** Те може да включват например налагане на глоба, временно ограничаване на обработването, изтриване на част от набора от данни, който е бил обработен незаконно, или, когато това не е възможно, в зависимост от конкретните факти, като се има предвид пропорционалността на мярката, разпореждане за изтриване на целия набор от данни, използван за разработване на модела на ИИ, и/или на самия модел на ИИ. Когато оценяват пропорционалността на предвидената мярка, надзорните органи могат да вземат предвид мерките, които могат да бъдат приложени от администратора за коригиране на неправомерността на първоначалното обработване (напр. повторно обучение).
115. ЕКЗД също така подчертава, че когато личните данни се обработват незаконно, субектите на данни могат да поискат заличаване на техните лични данни при спазване на условията, определени в член 17 от ОРЗД, и че надзорните органи могат да разпоредят заличаването на личните данни *ex officio*⁸⁸.
116. Когато оценяват дали дадена мярка е подходяща, необходима и пропорционална, НО може да вземат предвид, наред с други елементи, рисковете за субектите на данни, сериозността на нарушението, техническата и финансовата осъществимост на мярката, както и обема на съответните лични данни.

⁸⁶ Възможно е да се наложи да се вземат предвид специфични национални правила. Вж. например член 2-*decies* от италианския Кодекс за защита на данните (Законодателен декрет 196/2003), който постановява, че данните, обработвани в нарушение на правилата за защита на данните, не могат да бъдат използвани. Това не накърнява други национални правни рамки, като например наказателното право.

⁸⁷ Вж. в тази връзка съображение 129 от ОРЗД, както и Решение на Съда на ЕС от 26 септември 2024 г., дело C-768-21, *TR срещу Land Hessen* (ECLI:EU:C:2024:785), точка 37; Решение на Съда на ЕС от 7 декември 2023 г. по съединени дела C-26/22 и C-64/22, *SCHUFA Holding (Libération de reliquat de dette)* (ECLI:EU:C:2023:958), точка 57; и Решение на Съда на ЕС от 14 март 2024 г. по дело C-46/23, *Újpesti Polgármesteri Hivatal* (ECLI:EU:C:2024:239), точка 34.

⁸⁸ В тази връзка Становище 39/2021 на ЕКЗД относно това дали член 58, параграф 2, буква ж) от ОРЗД може да служи като правно основание за надзорния орган да разпреди *ex officio* изтриването на лични данни в ситуация, в която такова искане не е подадено от субекта на данните, параграф 28. Вж. също в това отношение Съд на ЕС, решение от 14 март 2024 г., дело C-46/23, *Újpesti Polgármesteri Hivatal* (ECLI:EU:C:2024:239), точка 42.

117. И накрая, ЕКЗД припомня, че мерките, предприети от надзорните органи съгласно ОРЗД, не засягат мерките, предприети от компетентните органи съгласно Акта за ИИ и/или съгласно други приложими правни рамки (напр. законодателство в областта на гражданската отговорност).
118. В следващите раздели ЕКЗД ще разгледа три сценария, обхванати от въпрос 4 от искането, при които разликите се състоят в това дали личните данни, обработвани за разработване на модела, се запазват в модела и/или дали последващото обработване се извършва от същия или друг администратор.

3.4.1 Сценарий 1. Администратор обработва лични данни незаконно, за да разработи модела, личните данни се запазват в модела и впоследствие се обработват от същия администратор (например при внедряването на модела)

119. Този сценарий се отнася до въпрос 4, подточка i) от искането, в случай че администраторът незаконно обработва лични данни (т.е. като не спазва член 5, параграф 1, буква а) от ОРЗД и член 6 от ОРЗД) с цел разработване на модел на ИИ, моделът на ИИ запазва информация, свързана с идентифицирано физическо лице или физическо лице, което може да бъде идентифицирано, и следователно не е анонимен. След това личните данни се обработват допълнително от същия администратор (например при внедряването на модела). Във връзка с този сценарий ЕКЗД представя следните съображения.
120. Правомощието на НО да налага коригиращи мерки по отношение на първоначалното обработване (както е обяснено в параграфи 113, 114 и 115 по-горе) по принцип ще има въздействие върху последващото обработване (напр. ако НО нареди на администратора да заличи личните данни, които са били обработени незаконно, тези коригиращи мерки няма да позволят на последния да обработва последващо личните данни, които са били предмет на мерките).
121. Що се отнася конкретно до въздействието на незаконосъобразното обработване на етапа на разработване върху последващото обработване (например на етапа на внедряване), ЕКЗД припомня, че надзорните органи са тези, които трябва да извършват анализ за всеки отделен случай, при който се вземат предвид конкретните обстоятелства.
122. **Дали етапите на разработване и внедряване включват отделни цели (и следователно представляват отделни дейности по обработване) и степента, до която липсата на правно основание за първоначалната дейност по обработване оказва въздействие върху законосъобразността на последващото обработване, следва да се оценява за всеки отделен случай, в зависимост от контекста на случая.**
123. Специално по отношение на правното основание на член 6, параграф 1, буква е) от ОРЗД например, когато последващото обработване се основава на легитимен интерес, фактът, че първоначалното обработване е било незаконно, следва да се вземе предвид при оценката на легитимния интерес (напр. по отношение на рисковете за субектите на данни или факта, че лицата може да не очакват такова последващо обработване). В тези случаи незаконосъобразността на обработването на етапа на разработване може да повлияе на законосъобразността на последващото обработване.

3.4.2 Сценарий 2. Администратор обработва лични данни незаконно, за да разработи модела, личните данни се запазват в модела и се обработват от друг администратор при внедряването на модела

124. Този сценарий се отнася до въпрос 4, буква и) от искането. Той се различава от сценарий 1 (в раздел 3.4.1 от настоящото становище), тъй като личните данни се обработват впоследствие от друг администратор при внедряването на модела на ИИ.
125. ЕКЗД припомня, че установяването на ролите, възложени на тези различни участници съгласно рамката за защита на данните, е съществена стъпка, за да се определи кои задължения съгласно ОРЗД се прилагат и кой носи отговорност за тези задължения, както и че при оценката на отговорностите на всяка от страните съгласно ОРЗД следва да се вземат предвид и ситуациите на съвместно администриране. Поради това забележките по-долу следва да се считат за общи елементи, които следва да се вземат предвид от надзорните органи, когато е уместно. Във връзка с този сценарий 2 ЕКЗД представя следните съображения.
126. На първо място следва да се припомни, че съгласно член 5, параграф 1, буква а) от ОРЗД, тълкуван в светлината на член 5, параграф 2 от ОРЗД, всеки администратор следва да гарантира законосъобразността на извършваното от него обработване и да може да я докаже. Поради това компетентните органи следва да оценят законосъобразността на обработването, извършено от i) администратора, който първоначално е разработил модела на ИИ; и ii) администратора, който е придобил модела на ИИ и обработва личните данни самостоятелно.
127. Второ, съображението, представено съгласно точки 113, 114, 115 по-горе, е от значение в настоящия случай, що се отнася до правомощието на НО да се намесват във връзка с първоначалното обработване. Член 17, параграф 1, буква г) от ОРЗД (изтриване на законно обработени данни) и член 19 от ОРЗД (задължение за уведомяване относно коригирането или изтриването на лични данни или ограничаване на обработването) могат, в зависимост от обстоятелствата по случая, също да бъдат от значение в този случай, например във връзка с уведомяването, което администраторът, разработващ модела, следва да извърши спрямо администратора, внедряващ модела.
128. Трето, във връзка с възможното въздействие на незаконността на първоначалното обработване върху последващото обработване, извършено от друг администратор, такава оценка следва да се извършва от НО за всеки отделен случай.
129. **За да се увери, че моделът на ИИ не е разработен чрез незаконно обработване на лични данни НО следва да вземат предвид това дали администраторът, който внедрява модела, е извършил подходяща оценка като част от задълженията си за отчетност⁸⁹, за да докаже спазването на член 5, параграф 1, буква а) и член 6 от ОРЗД.** При тази преценка от НО следва да се вземе предвид дали администраторът е оценил някои неизчерпателни критерии, като например източника на данните и дали моделът на ИИ е резултат от нарушение на ОРЗД, особено ако то е било установено от НО или от съда, така че администраторът, който внедрява модела, да не може да пренебрегне факта, че първоначалното обработване е било незаконно.
130. Администраторът следва да вземе предвид, например, дали данните произхождат от нарушение на сигурността на личните данни или дали обработването е било предмет на констатация за нарушение от страна на НО или съда. **Степента на оценката на администратора и нивото на детайлност, което НО очакват, може да варират в зависимост от различни фактори,**

⁸⁹ Член 5, параграф 2 от ОРЗД и член 24 от ОРЗД.

включително вида и степента на рисковете, пораждани от обработването, извършено в модела на ИИ по време на внедряването му по отношение на субектите на данни, чиито данни са използвани за разработването на модела.

131. ЕКЗД отбелязва, че съгласно Акта за ИИ от доставчиците на високорискови системи с ИИ се изисква да изготвят ЕС декларация за съответствие⁹⁰ и тази декларация трябва да съдържа изявление, че съответната система с ИИ е в съответствие със законодателството на ЕС за защита на данните⁹¹. ЕКЗД отбелязва, че такова лично деклариране може да не представлява окончателна констатация за съответствие съгласно ОРЗД. Въпреки това то може да бъде взето предвид от НО при разследването на конкретен модел на ИИ.
132. Същите съображения, изложени в точка 123 по-горе, също са от значение в настоящия случай. Когато надзорните органи проверяват дали и как администраторът е оценил целесъобразността на легитимния интерес като правно основание за обработването, което извършва, като част от оценката на легитимния интерес следва да се вземе предвид незаконността на първоначалното обработване, например като се оценят потенциалните рискове, които може да възникнат за субектите на данни, чиито лични данни са били неправомерно обработени за целите на разработването на модела. В рамките на сравнителния тест трябва надлежно да се разгледат различни аспекти както от техническо естество (напр. наличието на филтри или ограничения на достъпа, поставени по време на разработването на модела, които последващият администратор не може да заобиколи или промени и които биха могли да предотвратят достъпа до или разкриването на лични данни), така и от правно естество (напр. естеството и тежестта на незаконността на първоначалното обработване).

3.4.3 Сценарий 3. Администраторът незаконно обработва лични данни, за да разработи модела, след което гарантира, че те са анонимизирани, преди същият или друг администратор да започне друго обработване на лични данни в рамките на внедряването

133. Този сценарий е свързан с въпрос 4, подточка ii) от искането и се отнася до случай, в който администраторът неправомерно обработва лични данни, за да разработи модела на ИИ, но го прави по начин, който гарантира анонимността на личните данни, преди същият или друг администратор да инициира друго обработване на лични данни в рамките на внедряването. Първо ЕКЗД припомня, че НО имат компетентността и правомощието да се намесват по отношение на обработването, свързано с анонимизирането на модела, както и с обработването, извършвано по време на етапа на разработване. Следователно, надзорните органи могат, в зависимост от конкретните обстоятелства по случая, да наложат корективни мерки върху това първоначално обработване (както е обяснено в точки 113, 114 и 115 по-горе).
134. Ако може да се докаже, че последващото функциониране на модела на ИИ не води до обработване на лични данни, ЕКЗД счита, че ОРЗД няма да се прилага⁹². Следователно незаконосъобразността на първоначалното обработване не следва да оказва въздействие върху последващото функциониране на модела. ЕКЗД обаче подчертава, че самото твърдение за анонимност на модела не е достатъчно, за да го освободи от прилагането на ОРЗД, и отбелязва, че НО следва да го оценят, като вземат предвид, за всеки отделен случай, съображенията, предоставени от ЕКЗД в отговор на въпрос 1 от искането.

⁹⁰ Член 16, буква ж) и член 47 от Акта за ИИ.

⁹¹ Приложение V, точка 5 от Акта за ИИ.

⁹² Съображение 26 от ОРЗД.

135. Когато администраторите допълнително обработват лични данни, събрани по време на етапа на внедряване, след като моделът е анонимизиран, ОРЗД ще се прилага по отношение на тези дейности по обработване. В тези случаи, що се отнася до ОРЗД, законосъобразността на обработването, извършвано на етапа на внедряване, не следва да бъде засегната от незаконосъобразността на първоначалното обработване.

4 Заключение бележки

136. Настоящото становище е предназначено за всички НО и ще бъде публикувано съгласно член 64, параграф 5, буква б) от ОРЗД.

За Европейския комитет по защита на данните

Председател

Anu Talus