

Stanovisko Výboru podľa článku 64



Stanovisko 28/2024 k určitým aspektom ochrany údajov súvisiacim so spracúvaním osobných údajov v kontexte modelov umelej inteligencie

Prijaté 17. decembra 2024

Zhrnutie

Technológie umelej inteligencie vytvárajú mnoho príležitostí a prinášajú mnoho výhod v širokej škále odvetví a sociálnych činností.

Ochranou základného práva na ochranu údajov všeobecné nariadenie o ochrane údajov podporuje tieto príležitosti a presadzuje ďalšie základné práva EÚ vrátane práva na slobodu myslenia, prejavu a informácií, práva na vzdelanie alebo práva slobody podnikania. Týmto spôsobom je všeobecné nariadenie o ochrane údajov právnym rámcom podporujúcim zodpovedné inovácie.

V tejto súvislosti s prihliadnutím na otázky týkajúce sa ochrany údajov, ktoré tieto technológie vyvolávajú, írsky dozorný orgán požiadal Európsky výbor pre ochranu údajov (EDPB), aby vydal stanovisko k záležitostiam so všeobecným uplatnením podľa článku 64 ods. 2 všeobecného nariadenia o ochrane údajov. Žiadosť sa týka spracúvania osobných údajov v súvislosti s fázami vývoja a nasadzovania modelov umelej inteligencie. Konkrétnejšie, v žiadosti sa požadovalo: 1) kedy a akým spôsobom možno model umelej inteligencie považovať za „anonymný“; 2) ako môžu prevádzkovatelia preukázať vhodnosť oprávneného záujmu ako právneho základu vo fáze vývoja a 3) vo fáze nasadzovania a 4) aké sú dôsledky nezákonného spracúvania osobných údajov vo fáze vývoja modelu umelej inteligencie na následné spracúvanie alebo prevádzku modelu umelej inteligencie.

Pokiaľ ide o prvú otázku, v stanovisku sa uvádza, že tvrdenia o anonymite modelu umelej inteligencie by mali posudzovať príslušné dozorné orgány od prípadu k prípadu, keďže sa EDPB domnieva, že modely umelej inteligencie trénované pomocou osobných údajov nemožno vo všetkých prípadoch považovať za anonymné. Aby sa model umelej inteligencie považoval za anonymný, tak 1) pravdepodobnosť priamej (vrátane pravdepodobnostnej) extrakcie osobných údajov týkajúcich sa fyzických osôb, ktorých osobné údaje sa použili na vývoj modelu, ako aj 2) pravdepodobnosť úmyselného alebo neúmyselného získania takýchto osobných údajov z dopytov, by mala byť zanedbateľná, pričom sa zohľadnia „všetky prostriedky, pri ktorých je primeraná pravdepodobnosť, že ich využije“ prevádzkovateľ alebo iná osoba.

Na vykonanie posúdenia by dozorné orgány mali preskúmať dokumentáciu poskytnutú prevádzkovateľom s cieľom preukázať anonymitu modelu. V tejto súvislosti sa v stanovisku uvádza nenormatívny a neúplný zoznam metód, ktoré môžu prevádzkovatelia použiť pri preukazovaní anonymity, a teda ich dozorné orgány môžu zohľadniť pri posudzovaní tvrdenia prevádzkovateľa o anonymite. Zahŕňa to napríklad prístupy, ktoré prevádzkovatelia použili počas fázy vývoja s cieľom zabrániť alebo obmedziť získavanie osobných údajov používaných na trénovanie, znížiť ich identifikovateľnosť, zabrániť ich extrakcii alebo poskytnúť uistenie týkajúce sa najmodernejšej odolnosti voči útokom.

Pokiaľ ide o druhú a tretiu otázku, v stanovisku sa uvádzajú všeobecné úvahy, ktoré majú dozorné orgány zohľadniť pri posudzovaní toho, či sa prevádzkovatelia môžu spoľahnúť na oprávnený záujem ako na vhodný právny základ pre spracúvanie vykonávané v kontexte vývoja a nasadzovania modelov umelej inteligencie.

V stanovisku sa pripomína, že neexistuje hierarchia medzi právnymi základmi stanovenými vo všeobecnom nariadení o ochrane údajov a že je na prevádzkovateľoch, aby určili vhodný právny základ pre svoje spracovateľské činnosti. V stanovisku sa ďalej pripomína trojstupňový test, ktorý by sa mal vykonať pri posudzovaní použitia oprávneného záujmu ako právneho základu, t. j. 1) identifikácia oprávneného záujmu sledovaného prevádzkovateľom alebo treťou stranou; 2) analýza nevyhnutnosti

spracúvania na účely sledovaného oprávneného záujmu (oprávnených záujmov) (označované aj ako „test nevyhnutnosti“); a 3) posúdenie, či nad oprávneným záujmom (oprávnenými záujmami) neprevažujú záujmy alebo základné práva a slobody dotknutých osôb (označované aj ako „test vyvážení“).

Pokiaľ ide o prvý krok, v stanovisku sa pripomína, že záujem možno považovať za oprávnený, ak sú splnené tri nasledovné kumulatívne kritériá: záujem 1) je zákonný; 2) je jasne a presne formulovaný; a 3) je skutočný a prítomný (t. j. nie špekulatívny). Takýto záujem sa môže týkať napríklad vývoja modelu umelej inteligencie - vývoja služby konverzačného agenta na pomoc používateľom, alebo jeho nasadzovania - zlepšenia detekcie hrozieb v informačnom systéme.

Pokiaľ ide o druhý krok, v stanovisku sa pripomína, že posúdenie nevyhnutnosti zahŕňa zváženie: 1) či spracovateľská činnosť umožní sledovanie oprávneného záujmu a 2) či neexistuje menej rušivý spôsob sledovania tohto záujmu. Pri posudzovaní, či je splnená podmienka nevyhnutnosti, by dozorné orgány mali venovať osobitnú pozornosť množstvu spracúvaných osobných údajov a tomu, či je to primerané na sledovanie príslušného oprávneného záujmu, a to aj vzhľadom na zásadu minimalizácie údajov.

Pokiaľ ide o tretí krok, v stanovisku sa pripomína, že test vyvážení by sa mal vykonať s prihliadnutím na osobitné okolnosti každého prípadu. Ďalej poskytuje prehľad prvkov, ktoré môžu dozorné orgány zohľadniť pri posudzovaní toho, či nad záujmom prevádzkovateľa alebo tretej strany prevažujú záujmy, základné práva a slobody dotknutých osôb.

V rámci tretieho kroku sa v stanovisku upozorňuje na konkrétne riziká pre základné práva, ktoré sa môžu objaviť buď vo fáze vývoja, alebo vo fáze nasadzovania modelov umelej inteligencie. Takisto sa v ňom objasňuje, že spracúvanie osobných údajov, ktoré sa uskutočňuje počas fázy vývoja a nasadzovania modelov umelej inteligencie, môže mať vplyv na dotknuté osoby rôznymi spôsobmi, ktoré môžu byť pozitívne alebo negatívne. Na posúdenie takéhoto vplyvu môžu dozorné orgány zvážiť povahu údajov spracúvaných modelmi, kontext spracúvania a možné ďalšie dôsledky spracúvania.

V stanovisku sa okrem toho zdôrazňuje úloha primeraných očakávaní dotknutých osôb pri teste vyvážení. Môže to byť dôležité vzhľadom na zložitosť technológií používaných v modeloch umelej inteligencie a skutočnosť, že pre dotknuté osoby môže byť ťažké pochopiť rôznorodosť ich možného použitia, ako aj rôzne činnosti spracúvania. V tejto súvislosti môžu informácie poskytnuté dotknutým osobám, ako aj kontext spracúvania patriť k prvkom, ktoré sa majú zohľadniť pri posudzovaní toho, či dotknuté osoby môžu primerane očakávať, že ich osobné údaje budú spracúvané. Pokiaľ ide o kontext, môže to zahŕňať: či osobné údaje boli alebo neboli verejne dostupné, povahu vzťahu medzi dotknutou osobou a prevádzkovateľom (a či medzi nimi existuje prepojenie), povahu služby, kontext, v ktorom boli osobné údaje získané, zdroj, z ktorého boli údaje získané (t. j. webové sídlo alebo služba, kde boli osobné údaje získané, a nastavenia ochrany súkromia, ktoré ponúkajú), možné ďalšie použitia modelu a či dotknuté osoby skutočne vedia, že ich osobné údaje sú vôbec online.

V stanovisku sa takisto pripomína, že ak sa zdá, že záujmy, práva a slobody dotknutých osôb prevažujú nad oprávnenými záujmami, ktoré sleduje prevádzkovateľ alebo tretia strana, prevádzkovateľ môže zvážiť zavedenie zmierňujúcich opatrení na obmedzenie vplyvu spracúvania na tieto dotknuté osoby. Zmierňujúce opatrenia by sa nemali zamieňať s opatreniami, ktoré je prevádzkovateľ podľa zákona aj tak povinný prijať na zabezpečenie súladu so všeobecným nariadením o ochrane údajov. Okrem toho by opatrenia mali byť prispôsobené okolnostiam prípadu a charakteristikám modelu umelej inteligencie vrátane jeho zamýšľaného použitia. V tejto súvislosti sa v stanovisku uvádza nevyčerpávajúci zoznam príkladov zmierňujúcich opatrení v súvislosti s fázou vývoja (aj pokiaľ ide o extrahovanie údajov z webu) a fázou nasadzovania. Zmierňujúce opatrenia môžu podliehať rýchlemu

vývoju a mali by byť prispôsobené okolnostiam prípadu. Preto je na dozorných orgánoch, aby v jednotlivých prípadoch posúdili vhodnosť prijatých zmierňujúcich opatrení.

Pokiaľ ide o štvrtú otázku, v stanovisku sa vo všeobecnosti pripomína, že dozorné orgány majú diskrečnú právomoc posudzovať možné porušenia a vyberať vhodné, potrebné a primerané opatrenia s prihliadnutím na okolnosti každého jednotlivého prípadu. V stanovisku sa ďalej posudzujú tri scenáre.

Podľa scenára 1 sa osobné údaje uchovávali v modeli umelej inteligencie (čo znamená, že model nemožno považovať za anonymný, ako sa podrobne uvádza v prvej otázke) a následne ich spracúva ten istý prevádzkovateľ (napríklad v súvislosti s nasadzovaním modelu). V stanovisku sa uvádza, že to, či fázy vývoja a nasadzovania zahŕňajú samostatné účely (teda predstavujú samostatné spracovateľské činnosti) a rozsah, v akom neexistencia právneho základu pre pôvodnú spracovateľskú činnosť ovplyvňuje zákonnosť následného spracúvania, by sa mali posudzovať individuálne v závislosti od kontextu prípadu.

Podľa scenára 2 sa osobné údaje uchovávali v modeli a spracúva ich iný prevádzkovateľ v súvislosti s nasadzovaním modelu. V tejto súvislosti sa v stanovisku uvádza, že dozorné orgány by mali zohľadniť, či prevádzkovateľ, ktorý zavádza model, vykonal vhodné posúdenie v rámci svojich povinností v oblasti zodpovednosti na preukázanie súladu s článkom 5 ods. 1 písm. a) a článkom 6 všeobecného nariadenia o ochrane údajov s cieľom uistiť sa, že model umelej inteligencie nebol vyvinutý nezákonným spracúvaním osobných údajov. Toto posúdenie by malo zohľadňovať napríklad zdroj osobných údajov a skutočnosť a či spracúvanie vo fáze vývoja bolo predmetom zistenia porušenia, najmä ak ho určil dozorný orgán alebo súd, a malo by byť viac-menej podrobné v závislosti od rizík, ktoré vyvoláva spracúvanie vo fáze nasadzovania.

Podľa scenára 3 prevádzkovateľ nezákonne spracúva osobné údaje na účely vývoja modelu umelej inteligencie a potom zabezpečí ich anonymizáciu predtým, ako ten istý alebo iný prevádzkovateľ začne ďalšie spracúvanie osobných údajov v súvislosti s nasadzovaním modelu. V tejto súvislosti sa v stanovisku uvádza, že ak možno preukázať, že následné fungovanie modelu umelej inteligencie nezahŕňa spracúvanie osobných údajov, EDPB sa domnieva, že všeobecné nariadenie o ochrane údajov by sa neuplatňovalo. Nezákonnosť pôvodného spracúvania by preto nemala mať vplyv na následné fungovanie modelu. EDPB sa ďalej domnieva, že ak prevádzkovatelia následne spracúvajú osobné údaje získané počas fázy nasadzovania, po anonymizácii modelu by sa v súvislosti s týmito spracovateľskými operáciami všeobecné nariadenie o ochrane údajov uplatňovalo. V týchto prípadoch sa v stanovisku uvádza, že pokiaľ ide o všeobecné nariadenie o ochrane údajov, zákonnosť spracúvania vykonávaného vo fáze nasadzovania by nemala byť ovplyvnená nezákonnosťou prvotného spracúvania.

Obsah

1	Úvod	6
1.1	Zhrnutie skutočností	6
1.2	Prípustnosť žiadosti o stanovisko podľa článku 64 ods. 2 všeobecného nariadenia o ochrane údajov.....	8
2	Rozsah pôsobnosti a kľúčové pojmy	9
2.1	Rozsah pôsobnosti stanoviska	9
2.2	Kľúčové pojmy.....	11
2.3	Modely umelej inteligencie v kontexte stanoviska.....	12
3	O opodstatnenosti žiadosti	13
3.1	O povahe modelov umelej inteligencie v súvislosti s vymedzením osobných údajov	13
3.2	O okolnostiach, za ktorých by sa modely umelej inteligencie mohli považovať za anonymné a o súvisiacom preukázaní	15
3.2.1	Všeobecné úvahy týkajúce sa anonymizácie v danom kontexte	15
3.2.2	Prvky na vyhodnotenie zvyškovej pravdepodobnosti identifikácie.....	17
3.3	O vhodnosti oprávneného záujmu ako právneho základu pre spracúvanie osobných údajov v súvislosti s vývojom a nasadzovaním modelov umelej inteligencie	20
3.3.1	Všeobecné poznámky	20
3.3.2	Úvahy o troch krokoch posudzovania oprávneného záujmu v kontexte vývoja a nasadzovania modelov umelej inteligencie.....	22
3.4	O možnom vplyve nezákonného spracúvania pri vývoji modelu umelej inteligencie na zákonnosť následného spracúvania alebo prevádzky modelu umelej inteligencie.....	32
3.4.1	Scenár 1 Prevádzkovateľ neoprávnene spracúva osobné údaje na účely vývoja modelu, osobné údaje sa uchovávajú v modeli a následne ich spracúva ten istý prevádzkovateľ (napríklad v súvislosti s nasadením modelu).....	33
3.4.2	Scenár 2 Prevádzkovateľ neoprávnene spracúva osobné údaje na účely vývoja modelu, osobné údaje sa uchovávajú v modeli a spracúva ich iný prevádzkovateľ v súvislosti s nasadením modelu	34
3.4.3	Scenár 3 Prevádzkovateľ nezákonne spracúva osobné údaje na účely vývoja modelu, potom zabezpečí anonymizáciu modelu predtým, ako ten istý alebo iný prevádzkovateľ začne ďalšie spracúvanie osobných údajov v súvislosti s nasadením modelu	36
4	Záverečné pripomienky.....	36

Európsky výbor pre ochranu údajov

so zreteľom na článok 63 a článok 64 ods. 2 nariadenia Európskeho parlamentu a Rady (EÚ) 2016/679 z 27. apríla 2016 o ochrane fyzických osôb pri spracúvaní osobných údajov a o voľnom pohybe takýchto údajov, ktorým sa zrušuje smernica 95/46/ES (ďalej len „všeobecné nariadenie o ochrane údajov“),

so zreteľom na Dohodu o EHP, a najmä na jej prílohu XI a protokol 37, ktoré boli zmenené rozhodnutím Spoločného výboru EHP č. 154/2018 zo 6. júla 2018¹,

so zreteľom na článok 10 a článok 22 rokovacieho poriadku,

keďže:

1) Hlavnou úlohou Európskeho výboru pre ochranu údajov (ďalej len „**výbor**“ alebo „**EDPB**“) je zabezpečiť jednotné uplatňovanie všeobecného nariadenia o ochrane údajov v rámci celého Európskeho hospodárskeho priestoru (ďalej len „**EHP**“). V článku 64 ods. 2 všeobecného nariadenia o ochrane údajov sa stanovuje, že ktorýkoľvek dozorný orgán, predseda výboru alebo Komisia môže požiadať, aby akúkoľvek záležitosť so všeobecným uplatnením alebo s účinkami vo viac ako jednom členskom štáte EHP preskúmal výbor s cieľom získať stanovisko. Cieľom tohto stanoviska je preskúmať záležitosť so všeobecným uplatnením alebo s účinkami vo viac ako jednom členskom štáte EHP.

2) Stanovisko výboru sa prijme podľa článku 64 ods. 3 všeobecného nariadenia o ochrane údajov v spojení s článkom 10 ods. 2 rokovacieho poriadku výboru do ôsmich týždňov od prvého pracovného dňa po tom, čo predseda a príslušné dozorné orgány rozhodnú, že spis je úplný. Na základe rozhodnutia predsedu sa toto obdobie môže predĺžiť o ďalších šesť týždňov, pričom sa zohľadní zložitosť predmetu.

PRIJAL TOTO STANOVISKO

1 Úvod

1.1 Zhrnutie skutočností

1. Írsky dozorný orgán (ďalej len „**írsky dozorný orgán**“ alebo „**žiadajúci dozorný orgán**“) 4. septembra 2024 požiadal EDPB, aby vydal stanovisko podľa článku 64 ods. 2 všeobecného nariadenia o ochrane údajov v súvislosti s modelmi umelej inteligencie a spracúvaním osobných údajov (ďalej len „**žiadosť**“).
2. Predseda výboru a írsky dozorný orgán považovali spis za úplný 13. septembra 2024. V nasledujúci pracovný deň, 16. septembra 2024, sekretariát EDPB uverejnil spis. Vzhľadom na zložitosť záležitosti sa predseda rozhodol predĺžiť právnu lehotu v súlade s článkom 64 ods. 3 všeobecného nariadenia o ochrane údajov a článkom 10 ods. 4 rokovacieho poriadku výboru.
3. Žiadosť sa týka určitých prvkov tréningu, aktualizácie, vývoja a prevádzky modelov umelej inteligencie, pri ktorých osobné údaje tvoria súčasť príslušného súboru údajov. Írsky dozorný orgán zdôrazňuje, že žiadosť sa týka kľúčových otázok, ktoré majú veľký vplyv na dotknuté osoby a

¹ Odkazy na „členské štáty“ uvedené v tomto stanovisku sa majú chápať ako odkazy na „členské štáty EHP“. Odkazy na „Úniu“ uvedené v tomto stanovisku sa majú chápať ako odkazy na „EHP“.

prevádzkovateľov v EHP, a že v tejto fáze neexistuje harmonizované stanovisko medzi vnútroštátnymi dozornými orgánmi². Terminológia, ktorá sa bude používať na účely tohto stanoviska, je uvedená ďalej v oddieloch 2.2 a 2.3.

4. Írsky dozorný orgán položil tieto otázky:

Otázka 1: Považuje sa konečný model umelej inteligencie, ktorý bol trénovaný s použitím osobných údajov, vo všetkých prípadoch za model, ktorý nespĺňa definíciu osobných údajov (ako sa uvádza v článku 4 ods. 1 nariadenia o ochrane údajov)?

Ak je odpoveď na otázku 1 kladná:

- i. V ktorej fáze spracovateľských operácií vedúcich k modelu umelej inteligencie sa osobné údaje už nespracúvajú?
 - a) Ako možno preukázať, že model umelej inteligencie nespracúva osobné údaje?
- ii. Existujú nejaké faktory, ktoré by spôsobili, že fungovanie konečného modelu umelej inteligencie sa už nebude považovať za anonymné?
 - a) Ak áno, ako možno preukázať opatrenia prijaté na zmiernenie, prevenciu alebo ochranu pred týmito faktormi (aby sa zabezpečilo, že model umelej inteligencie nespracúva osobné údaje)?

Ak je odpoveď na otázku 1 záporná:

- i. Za akých okolností to môže nastať?
 - a) Ak je to tak, ako možno preukázať kroky, ktoré sa prijali na zabezpečenie toho, aby model umelej inteligencie nespracúval osobné údaje?

Otázka 2: Ak sa prevádzkovateľ spolieha na oprávnené záujmy ako na právny základ pre spracúvanie osobných údajov s cieľom vytvoriť, aktualizovať a/alebo vyvinúť model umelej inteligencie, ako by mal tento prevádzkovateľ preukázať vhodnosť oprávnených záujmov ako právneho základu, a to vo vzťahu k spracúvaniu údajov tretej strany, ako aj údajov prvej strany?

- i. Aké úvahy by mal tento prevádzkovateľ zohľadniť, aby sa zabezpečilo, že záujmy dotknutých osôb, ktorých osobné údaje sa spracúvajú, sú vhodne vyvážené so záujmami tohto prevádzkovateľa v kontexte:
 - a) údajov tretej strany
 - b) údajov prvej strany

Otázka 3: Po tréningu, ak sa prevádzkovateľ spolieha na oprávnené záujmy ako na právny základ pre spracúvanie osobných údajov v rámci modelu umelej inteligencie alebo systému umelej inteligencie, ktorého súčasťou je model umelej inteligencie, ako by mal prevádzkovateľ preukázať vhodnosť oprávnených záujmov ako právneho základu?

Otázka 4: Ak sa zistí, že model umelej inteligencie bol vytvorený, aktualizovaný alebo vyvinutý s použitím nezákonne spracúvaných osobných údajov, aký je jeho prípadný vplyv na zákonnosť ďalšieho alebo následného spracúvania alebo prevádzky modelu umelej inteligencie, a to buď samostatne, alebo ako súčasť systému umelej inteligencie, ak:

² Žiadosť, s. 1.

- i. model umelej inteligencie, či už samostatne alebo ako súčasť systému umelej inteligencie, spracúva osobné údaje?
- ii. ani model umelej inteligencie, ani model umelej inteligencie ako súčasť systému umelej inteligencie nespracúvajú osobné údaje?

1.2 Prípustnosť žiadosti o stanovisko podľa článku 64 ods. 2 všeobecného nariadenia o ochrane údajov

- 5. V článku 64 ods. 2 všeobecného nariadenia o ochrane údajov sa stanovuje, že ktorýkoľvek dozorný orgán môže požiadať, aby akúkoľvek záležitosť so všeobecným uplatnením alebo s účinkami vo viac ako jednom členskom štáte preskúmal výbor s cieľom získať stanovisko.
- 6. Žiadajúci dozorný orgán adresoval EDPB otázky týkajúce sa aspektov ochrany údajov v súvislosti s modelmi umelej inteligencie. V žiadosti sa uvádza, že hoci mnohé organizácie v súčasnosti používajú modely umelej inteligencie vrátane veľkých jazykových modelov („large language models“ alebo „LLMs“), ich prevádzka, tréning a používanie vyvolávajú „niekoľko rozsiahlych obáv týkajúcich sa ochrany údajov“³, ktoré „majú vplyv na dotknuté osoby v celej EÚ/EHP“⁴.
- 7. Žiadosť v podstate nastoľuje otázky týkajúce sa i) uplatňovania pojmu osobných údajov; ii) zásady zákonnosti s osobitným zreteľom na právny základ oprávneného záujmu v kontexte modelov umelej inteligencie; ako aj iii) dôsledkov nezákonného spracúvania osobných údajov vo fáze vývoja modelov umelej inteligencie na následné spracúvanie alebo prevádzku modelu.
- 8. Výbor sa domnieva, že sa táto žiadosť týka „záležitosti so všeobecným uplatnením“ v zmysle článku 64 ods. 2 všeobecného nariadenia o ochrane údajov. Vec sa týka najmä výkladu a uplatňovania článku 4 ods. 1, článku 5 ods. 1 písm. a) a článku 6 všeobecného nariadenia o ochrane údajov v súvislosti so spracúvaním osobných údajov pri vývoji a nasadzovaní modelov umelej inteligencie. Ako zdôraznil žiadajúci dozorný orgán, uplatňovanie týchto ustanovení na modely umelej inteligencie vyvoláva systémové, abstraktné a nové otázky⁵. Rýchly vývoj a nasadzovanie modelov umelej inteligencie zo strany čoraz väčšieho počtu organizácií vyvoláva osobitné otázky a, ako sa uvádza v žiadosti, „EDPB bude mať veľký prospech z dosiahnutia spoločnej pozície k záležitostiam, ktoré sú predmetom tejto žiadosti, pričom takéto záležitosti sú kľúčové pre plánovanú prácu EDPB v krátkodobom a strednodobom horizonte“⁶. Okrem toho technológie umelej inteligencie vytvárajú mnohé príležitosti a výhody v širokej škále odvetví a spoločenských aktivít. Všeobecné nariadenie o ochrane údajov je okrem toho právnym rámcom, ktorý podporuje zodpovedné inovácie. Z toho vyplýva, že existuje všeobecný záujem na vykonaní tohto posúdenia vo forme stanoviska EDPB s cieľom zabezpečiť konzistentné uplatňovanie určitých ustanovení všeobecného nariadenia o ochrane údajov v kontexte modelov umelej inteligencie.
- 9. Druhá podmienka uvedená v článku 64 ods. 2 všeobecného nariadenia o ochrane údajov sa týka záležitostí „s účinkami vo viac ako jednom členskom štáte“. EDPB pripomína, že pojem „účinky“ sa má

³ Žiadosť, s. 1.

⁴ Tamže.

⁵ Žiadosť, s. 2.

⁶ Žiadosť, s. 1. Ako sa uvádza v pracovnom programe EDPB na roky 2024 - 2025, prijatom 8. októbra 2024, ktorý je k dispozícii na adrese https://www.edpb.europa.eu/system/files/2024-10/edpb_work_programme_2024-2025_en.pdf, EDPB plánuje vydať, okrem iného, usmernenia o anonymizácii, pseudonymizácii a vyradovaní údajov v kontexte generatívnej umelej inteligencie.

vykladať *lato sensu*, a teda nie je obmedzený len na právne účinky⁷. Keďže sa čoraz viac modelov umelej inteligencie trénuje a používa v čoraz väčšom počte organizácií v EHP, majú vplyv na veľký počet dotknutých osôb v celom EHP, z ktorých niektoré už vyjadrili obavy príslušnému dozornému orgánu⁸. EDPB sa preto domnieva, že vec, ktorú predložil žiadajúci dozorný orgán, spĺňa aj túto podmienku.

10. Žiadosť obsahuje písomné odôvodnenie týkajúce sa podkladov a motivácií na predkladanie otázok výboru, a to aj v súvislosti s príslušným právnym rámcom. Výbor sa preto domnieva, že žiadosť je odôvodnená v súlade s článkom 10 ods. 3 rokovacieho poriadku EDPB.
11. Podľa článku 64 ods. 3 všeobecného nariadenia o ochrane údajov⁹ EDPB nevydá stanovisko, ak už k danej záležitosti stanovisko vydal. EDPB k rovnakej záležitosti stanovisko a ešte neposkytol odpovede na otázky vyplývajúce z tejto žiadosti.
12. Z týchto dôvodov sa výbor domnieva, že žiadosť je prípustná a otázky, ktoré z nej vyplývajú, by sa mali analyzovať v tomto stanovisku (ďalej len „**stanovisko**“) prijatom podľa článku 64 ods. 2 všeobecného nariadenia o ochrane údajov.

2 Rozsah pôsobnosti a kľúčové pojmy

2.1 Rozsah pôsobnosti stanoviska

13. Výbor súhlasí so žiadajúcim dozorným orgánom, že z hľadiska ochrany údajov vývoj a nasadzovanie modelov umelej inteligencie vyvolávajú základné otázky ochrany údajov. Otázky sa týkajú najmä toho: i) kedy a ako možno model umelej inteligencie považovať za „anonymný“ (otázka 1 žiadosti); ii) ako môžu prevádzkovatelia preukázať vhodnosť oprávneného záujmu ako právneho základu vo fázach vývoja (otázka 2 žiadosti) a nasadzovania (otázka 3 žiadosti) a iii) či má nezákonné spracúvanie osobných údajov vo fáze vývoja dôsledky na zákonnosť následného spracúvania alebo prevádzky modelu umelej inteligencie (otázka 4 žiadosti).
14. EDPB pripomína, že dozorné orgány sú zodpovedné za monitorovanie uplatňovania všeobecného nariadenia o ochrane údajov a mali by prispievať k jeho konzistentnému uplatňovaniu v celej Únii¹⁰. Je preto v právomoci dozorných orgánov vyšetrovať konkrétne modely umelej inteligencie a pri tom vykonávať posúdenia jednotlivých prípadov.
15. Toto stanovisko poskytuje príslušným dozorným orgánom rámec na posúdenie konkrétnych prípadov, v ktorých by sa vyskytli (niektoré) otázky uvedené v žiadosti. Toto stanovisko nemá za cieľ byť vyčerpávajúce, ale skôr poskytnúť všeobecné úvahy o výklade príslušných ustanovení, ktoré by príslušné dozorné orgány mali v čo najväčšej miere zohľadniť pri využívaní svojich vyšetrovacích právomocí. Hoci je toto stanovisko určené príslušným dozorným orgánom a týka sa ich činností a právomocí, nie sú ním dotknuté povinnosti prevádzkovateľov a sprostredkovateľov podľa všeobecného nariadenia o ochrane údajov. Najmä podľa zásady zodpovednosti zakotvenej v článku 5 ods. 2 všeobecného nariadenia o ochrane údajov sú prevádzkovatelia zodpovední za všetky zásady týkajúce sa ich spracúvania osobných údajov a musia byť schopní preukázať ich dodržiavanie.

⁷EDPB, interný dokument č. 3/2019 o interných usmerneniach k článku 64 ods. 2 všeobecného nariadenia o ochrane údajov, prijatý 8. októbra 2019, bod 15, k dispozícii na adrese https://www.edpb.europa.eu/system/files/2022-07/internaledpb_document_201903_art64.2_en.pdf.

⁸ Žiadosť, s. 1 – 2.

⁹ Článok 64 ods. 3 všeobecného nariadenia o ochrane údajov a článok 10 ods. 4 rokovacieho poriadku EDPB.

¹⁰ Článok 51 ods. 1 všeobecného nariadenia o ochrane údajov a článok 51 ods. 2 všeobecného nariadenia o ochrane údajov.

16. V niektorých prípadoch sa v stanovisku môžu uviesť niektoré príklady, ale vzhľadom na široký rozsah otázok zahrnutých v žiadosti, ako aj rôzne typy modelov umelej inteligencie, na ktoré sa žiadosť vzťahuje, sa v tomto stanovisku nebudú brať do úvahy všetky možné scenáre. Technológie spojené s modelmi umelej inteligencie podliehajú rýchlemu vývoju. Preto by sa úvahy EDPB v tomto stanovisku mali interpretovať s ohľadom na túto skutočnosť.
17. **V tomto stanovisku sa neanalyzujú nižšie uvedené ustanovenia, ktoré môžu stále zohrávať dôležitú úlohu pri posudzovaní požiadaviek na ochranu údajov uplatniteľných na modely umelej inteligencie:**
- **Spracúvanie osobitných kategórií údajov:** EDPB pripomína zákaz uvedený v článku 9 ods. 1 všeobecného nariadenia o ochrane údajov, pokiaľ ide o spracúvanie osobitných kategórií údajov, a obmedzené výnimky článku 9 ods. 2 všeobecného nariadenia o ochrane údajov¹¹. V tejto súvislosti Súdny dvor Európskej únie (ďalej len „SDEÚ“) ďalej objasnil, že „*ak je predmetom takýchto operácií súbor údajov, ktorý obsahuje tak citlivé, ako aj necitlivé údaje, a najmä ak sa získava ako celok bez toho, aby bolo možné údaje v čase tohto získavania od seba oddeliť musí sa spracúvanie tohto súboru údajov považovať za zakázané v zmysle článku 9 ods. 1 všeobecného nariadenia o ochrane údajov, pokiaľ obsahuje aspoň jeden citlivý údaj a neuplatňuje sa žiadna z výnimiek uvedených v článku 9 ods. 2 tohto nariadenia*“¹². SDEÚ ďalej zdôraznil, že „*na účely uplatnenia výnimky stanovenej v článku 9 ods. 2 písm. e) všeobecného nariadenia o ochrane údajov treba overiť, či dotknutá osoba výslovne a jednoznačným potvrdzujúcim úkonom zamýšľala sprístupniť predmetné osobné údaje širokej verejnosti*“¹³. Tieto úvahy by sa mali zohľadniť pri spracúvaní osobných údajov v kontexte modelov umelej inteligencie, ktoré zahŕňajú osobitné kategórie údajov.
 - **Automatizované rozhodovanie vrátane profilovania:** Spracovateľské operácie vykonávané v kontexte modelov umelej inteligencie môžu patriť do rozsahu pôsobnosti článku 22 všeobecného nariadenia o ochrane údajov, ktorým sa prevádzkovateľom ukladajú dodatočné povinnosti a dotknutým osobám sa poskytujú dodatočné záruky. EDPB v tejto súvislosti pripomína svoje usmernenia k automatizovanému individuálnemu rozhodovaniu a profilovaniu na účely nariadenia 2016/679¹⁴.
 - **Zlučiteľnosť účelov:** V článku 6 ods. 4 všeobecného nariadenia o ochrane údajov sa pre určité právne základy stanovujú kritériá, ktoré musí prevádzkovateľ zohľadniť, aby zistil, či je spracúvanie na iný účel zlučiteľné s účelom, na ktorý sa osobné údaje pôvodne získali. Toto ustanovenie môže byť relevantné v kontexte vývoja a nasadzovania modelov umelej inteligencie a jeho uplatniteľnosť by mali posúdiť dozorné orgány.
 - **Posúdenia vplyvu na ochranu údajov** (článok 35 všeobecného nariadenia o ochrane údajov): Posúdenie vplyvu na ochranu údajov je dôležitým prvkom zodpovednosti, ak je pravdepodobné,

¹¹ Pozri aj správu EDPB o práci, ktorú vykonala pracovná skupina pre ChatGPT, prijatú 23. mája 2024, bod 18: „Pokiaľ ide o spracúvanie osobitných kategórií osobných údajov, musí sa okrem toho uplatniť jedna z výnimiek uvedených v článku 9 ods. 2, aby bolo spracúvanie zákonné. Jednou z týchto výnimiek môže byť v zásade článok 9 ods. 2 písm. e) všeobecného nariadenia o ochrane údajov. Samotná skutočnosť, že osobné údaje sú verejne prístupné, však neznamená, že „dotknutá osoba tieto údaje zjavne zverejnila“ [...].“

¹² Rozsudok SDEÚ zo 4. júla 2023, vec C-252/21, *Meta v. Bundeskartellamt* (ECLI:EU:C:2023:537), bod 89.

¹³ Rozsudok SDEÚ zo 4. júla 2023, vec C-252/21, *Meta v. Bundeskartellamt* (ECLI:EU:C:2023:537), bod 77.

¹⁴ Usmernenia pracovnej skupiny zriadenej podľa článku 29 (WP29) k automatizovanému individuálnemu rozhodovaniu a profilovaniu na účely nariadenia 2016/679, naposledy revidované a prijaté 6. februára 2018, schválené Európskym výborom pre ochranu údajov 25. mája 2018. Pozri tiež rozsudok SDEÚ zo 7. decembra 2023, vec C-634/21, *SCHUFA Holding a i.* (ECLI:EU:C:2023:957).

že spracúvanie v kontexte modelov umelej inteligencie bude mať za následok vysoké riziko pre práva a slobody fyzických osôb¹⁵.

- **Zásada špecificky navrhutej ochrany údajov** (článok 25 ods. 1 všeobecného nariadenia o ochrane údajov): Špecificky navrhnutá ochrana údajov je základnou zárukou, ktorú majú posudzovať dozorné orgány v súvislosti s vývojom a nasadzovaním modelu umelej inteligencie.

2.2 Kľúčové pojmy

18. Na úvod by EDPB chcel poskytnúť vysvetlenia týkajúce sa terminológie a pojmov, ktoré používa v celom tomto stanovisku, a len na účely tohto stanoviska:

- **„Údaje prvej strany“** sa vzťahujú na osobné údaje, ktoré prevádzkovateľ získal od dotknutých osôb.
- **„Údaje tretej strany“** sa vzťahujú na osobné údaje, ktoré prevádzkovatelia nezískali od dotknutých osôb, ale získali ich alebo ich dostali od tretej strany, napríklad od sprostredkovateľa údajov alebo prostredníctvom extrakcie dát z webu („web scraping“).
- **„Extrakcia dát z webu“** („web scraping“) je bežne používaná technika získavania informácií z verejne dostupných online zdrojov. Informácie extrahované napríklad zo služieb, ako sú spravodajské kanály, sociálne médiá, diskusné fóra a osobné webové stránky, môžu obsahovať osobné údaje.
- V žiadosti sa odkazuje na **„životný cyklus“ modelov umelej inteligencie**, ako aj na rôzne fázy týkajúce sa okrem iného „vytvorenia“, „vývoja“, „trénovania“, „aktualizácie“, „doladenia“, „prevádzky“ alebo „následného trénovania“ modelov umelej inteligencie. EDPB uznáva, že v závislosti od okolností sa takéto fázy môžu uskutočniť pri vývoji a nasadzovaní modelov umelej inteligencie a môžu zahŕňať spracúvanie osobných údajov na rôzne účely spracúvania. Napriek tomu EDPB na účely tohto stanoviska považuje za dôležité zjednodušiť kategorizáciu pravdepodobných fáz. Na účely tohto stanoviska sa preto EDPB odvoláva na **„fázu vývoja“** a na **„fázu nasadzovania“**. Vývoj modelu umelej inteligencie zahŕňa všetky fázy pred akýmkoľvek zavedením modelu umelej inteligencie a zahŕňa okrem iného vývoj kódov, získavanie tréningových osobných údajov, predbežné spracúvanie tréningových osobných údajov a trénovanie. Nasadenie modelu umelej inteligencie sa vzťahuje na všetky fázy súvisiace s používaním modelu umelej inteligencie a môže zahŕňať všetky operácie vykonané po fáze vývoja. EDPB si je aj naďalej vedomý rôznorodosti prípadov použitia a ich potenciálnych dôsledkov z hľadiska spracúvania osobných údajov. Dozorné orgány by preto mali zvážiť, či sú pripomienky uvedené v tomto stanovisku relevantné pre spracúvanie, ktoré posudzujú.
- EDPB tiež zdôrazňuje, že v prípade potreby sa pojem **„trénovanie“** vzťahuje na časť fázy vývoja, v ktorej sa modely umelej inteligencie učia z údajov, aby mohli vykonávať svoju zamýšľanú úlohu (ako je vysvetlené v ďalšej časti tohto stanoviska).
- Pojem a rozsah **modelov umelej inteligencie**, ako ho chápe EDPB na účely tohto stanoviska, je bližšie špecifikovaný v nasledujúcej osobitnej časti.

¹⁵ WP29, Usmernenia týkajúce sa posúdenia vplyvu na ochranu údajov a stanovenie toho, či spracúvanie „pravdepodobne povedie k vysokému riziku“ na účely nariadenia 2016/679, revidované a prijaté 4. októbra 2017, schválené EDPB 25. mája 2018.

2.3 Modely umelej inteligencie v kontexte stanoviska

19. V akte EÚ o umelej inteligencii (ďalej len „**akt o umelej inteligencii**“) sa „systém AI“¹⁶ vymedzuje ako „*strojový systém, ktorý je dizajnovaný na prevádzku s rôznymi úrovňami autonómnosti, ktorý môže po nasadení prejavovať adaptabilitu a ktorý pre explicitné alebo implicitné ciele odvodzuje zo vstupov, ktoré dostáva, spôsob generovania výstupov, ako sú predpovede, obsah, odporúčania alebo rozhodnutia, ktoré môžu ovplyvniť fyzické alebo virtuálne prostredie*“¹⁷. V odôvodnení 12 aktu o umelej inteligencii sa ďalej vysvetľuje pojem „systém AI“. Kľúčovou charakteristikou systémov umelej inteligencie je preto ich spôsobilosť odvodzovať. Medzi techniky, ktoré umožňujú odvodzovanie pri budovaní systému umelej inteligencie, patria strojové učenie, a prístupy založené na logike a vedomostiach.
20. Na druhej strane, „modely umelej inteligencie“ sú v zákone o umelej inteligencii definované len nepriamo: „*Hoci sú modely AI základnými komponentmi systémov AI, samy osebe nepredstavujú systémy AI. Modely AI si vyžadujú pridanie ďalších komponentov, ako je napríklad používateľské rozhranie, aby sa z nich stali systémy AI. Modely AI sú zvyčajne integrované do systémov AI a tvoria ich súčasť*“¹⁸.
21. EDPB rozumie, že vymedzenie modelu umelej inteligencie navrhnuté v žiadosti je užšie ako vymedzenie z aktu o umelej inteligencii, keďže sa v ňom odkazuje na „model umelej inteligencie“ ako „*zahŕňajúci výrobok vyplývajúci z mechanizmov tréningovania, ktoré sa uplatňujú na súbor tréningových údajov v kontexte umelej inteligencie, strojového učenia, hĺbkového učenia alebo iných súvisiacich kontextov spracúvania*“, a ďalej spresňuje, že „*Tento pojem sa vzťahuje na modely umelej inteligencie, ktoré sú určené na ďalšie tréningovanie, doladovanie a/alebo vývoj, ako aj na modely umelej inteligencie, ktoré nie sú.*“¹⁹
22. Na základe toho EDPB prijal toto stanovisko za predpokladu, že systém umelej inteligencie sa pri plnení svojho zamýšľaného cieľa bude spoliehať na model umelej inteligencie tým, že ho začlení do väčšieho rámca (napr. systém umelej inteligencie pre zákaznícke služby by mohol používať model umelej inteligencie trénovaný na základe historických konverzačných údajov s cieľom poskytnúť odpovede na otázky používateľov).
23. Okrem toho, modely umelej inteligencie (alebo „**modely**“) relevantné pre toto stanovisko, sú modely vyvinuté prostredníctvom tréningového procesu. Takýto tréningový proces je súčasťou fázy vývoja, v ktorej sa modely učia z údajov, aby mohli plniť zamýšľanú úlohu. Tréningový proces si preto vyžaduje súbor údajov, na základe ktorého model identifikuje vzory a „učí“ sa ich. V týchto prípadoch model použije rôzne techniky na vytvorenie znázornenia znalostí extrahovaných z tréningového súboru údajov. Týka sa to najmä strojového učenia.
24. V praxi je každý model umelej inteligencie algoritmom, ktorého fungovanie je určené súborom prvkov. Napríklad modely hĺbkového učenia majú často podobu neurónovej siete s viacerými vrstvami pozostávajúcimi z uzlov prepojených hranami, ktoré majú váhy, ktoré sa počas tréningovania upravujú, aby sa naučili vzťahy medzi vstupmi a výstupmi. Charakteristiky jednoduchého modelu hĺbkového učenia by boli nasledovné: i) typ a veľkosť každej vrstvy, ii) váha priradená každej hrane (niekedy

¹⁶ Nariadenie Európskeho parlamentu a Rady (EÚ) 2024/1689 z 13. júna 2024, ktorým sa stanovujú harmonizované pravidlá v oblasti umelej inteligencie a ktorým sa menia nariadenia (ES) č. 300/2008, (EÚ) č. 167/2013, (EÚ) č. 168/2013, (EÚ) 2018/858, (EÚ) 2018/1139 a (EÚ) 2019/2144 a smernice 2014/90/EÚ, (EÚ) 2016/797 a (EÚ) 2020/1828 (akt o umelej inteligencii).

¹⁷ Článok 3 ods. 1 aktu o umelej inteligencii.

¹⁸ Odôvodnenie 97 aktu o umelej inteligencii.

¹⁹ Žiadosť, s. 3.

nazývané „parametre“), iii) aktivačné funkcie²⁰ medzi vrstvami a prípadne iv) iné operácie, ktoré sa môžu uskutočniť medzi vrstvami. Napríklad pri tréňovaní jednoduchého modelu hlbokého učenia na klasifikáciu obrázkov sa vstupy („**pixels obrázku**“) priradia k výstupom a váhy sa môžu upraviť tak, aby vo väčšine prípadov poskytovali správny výstup.

25. Medzi ďalšie príklady modelov hlbokého učenia patria veľké jazykové modely („LLMs“) a generatívna umelá inteligencia, ktoré sa používajú napr. na vytváranie obsahu podobného ľudskej činnosti a vytváranie nových údajov.
26. **Na základe uvedených úvah a v súlade so žiadosťou sa rozsah pôsobnosti tohto stanoviska vzťahuje len na podmnožinu modelov umelej inteligencie, ktoré sú výsledkom tréňovania takýchto modelov s osobnými údajmi.**

3 O opodstatnenosti žiadosti

3.1 O povahe modelov umelej inteligencie v súvislosti s vymedzením osobných údajov

27. V článku 4 ods. 1 všeobecného nariadenia o ochrane údajov sa osobné údaje definujú ako „*akékoľvek informácie týkajúce sa identifikovanej alebo identifikovateľnej fyzickej osoby*“ (t. j. dotknutej osoby). Okrem toho sa v odôvodnení 26 všeobecného nariadenia o ochrane údajov stanovuje, že zásady ochrany údajov by sa nemali uplatňovať na anonymné informácie, konkrétne na informácie, ktoré sa nevzťahujú na identifikovanú alebo identifikovateľnú fyzickú osobu, pričom sa zohľadňujú „*všetky prostriedky, pri ktorých existuje primeraná pravdepodobnosť, že ich prevádzkovateľ alebo akákoľvek iná osoba využije*“. To zahŕňa: i) údaje, ktoré sa nikdy netýkali identifikovanej alebo identifikovateľnej fyzickej osoby, a ii) osobné údaje, ktoré boli anonymizované takým spôsobom, že dotknutá osoba nie je alebo už nie je identifikovateľná.
28. Otázku 1²¹ žiadosti preto možno zodpovedať analýzou toho, či by sa model umelej inteligencie, ktorý je výsledkom tréňovania zahŕňajúceho spracúvanie osobných údajov, mal vo všetkých prípadoch považovať za anonymný. Na základe formulovania otázky bude EDPB v tejto časti odkazovať na proces „tréňovania“ modelu umelej inteligencie.
29. EDPB by v prvom rade chcel uviesť nasledovné všeobecné úvahy. Modely umelej inteligencie, bez ohľadu na to, či sú tréňované na základe osobných údajov alebo nie, sú zvyčajne navrhnuté na vytváranie predpovedí alebo vyvodzovanie záverov, t. j. sú navrhnuté na odvodzovanie. Okrem toho sú modely umelej inteligencie tréňované pomocou osobných údajov často navrhnuté tak, aby robili závery o iných osobách, ako sú osoby, ktorých osobné údaje boli použité na tréňovanie modelu umelej inteligencie. Niektoré modely umelej inteligencie sú však osobitne navrhnuté tak, aby poskytovali osobné údaje týkajúce sa jednotlivcov, ktorých osobné údaje sa použili na tréňovanie modelu, alebo aby nejakým spôsobom takéto údaje sprístupnili. V týchto prípadoch budú takéto modely umelej inteligencie inherentne (a zvyčajne nevyhnutne) obsahovať informácie týkajúce sa identifikovanej alebo identifikovateľnej fyzickej osoby, a teda budú zahŕňať spracúvanie osobných údajov. Preto tieto typy modelov umelej inteligencie nemožno považovať za anonymné. To by bol napríklad prípad i)

²⁰ T. j. funkcie, ktoré na základe vstupov a váh vypočítavajú výstup neurónového uzla, ktorý sa potom odošle do ďalšej vrstvy neurónovej siete.

²¹ „Považuje sa konečný model umelej inteligencie, ktorý bol tréňovaný s použitím osobných údajov, vo všetkých prípadoch za model, ktorý nespĺňa definíciu osobných údajov (ako sa uvádza v článku 4 ods. 1 všeobecného nariadenia o ochrane údajov)?“

generatívneho modelu doladeného na základe hlasových záznamov jednotlivca tak, aby napodobňoval jeho hlas, alebo ii) akéhokoľvek modelu navrhnutého tak, aby na výzvu na poskytnutie informácií týkajúcich sa konkrétnej osoby odpovedal osobnými údajmi získanými na základe tréningu.

30. Na základe uvedených úvah sa EDPB v odpovedi na otázku č. 1 žiadosti zameriava na situáciu modelov umelej inteligencie, ktoré nie sú navrhnuté tak, aby poskytovali osobné údaje súvisiace s tréningovými údajmi.
31. EDPB sa domnieva, že aj keď model umelej inteligencie nebol zámerne navrhnutý tak, aby z tréningových údajov vytváral informácie týkajúce sa identifikovanej alebo identifikovateľnej fyzickej osoby, informácie zo súboru tréningových údajov vrátane osobných údajov môžu zostať „absorbované“ v parametroch modelu, konkrétne reprezentované prostredníctvom matematických objektov. Môžu sa líšiť od pôvodných tréningových údajov, stále však môžu uchovávať pôvodné informácie o týchto údajoch, ktoré môžu byť v konečnom dôsledku extrahovateľné alebo inak priamo alebo nepriamo získané z modelu. Vždy, keď informácie týkajúce sa identifikovaných alebo identifikovateľných osôb, ktorých osobné údaje sa použili na tréning modelu, možno získať z modelu umelej inteligencie spôsobom, pri ktorom je primerane pravdepodobné, že sa použije, možno dospieť k záveru, že takýto model nie je anonymný.
32. V tejto súvislosti sa v žiadosti uvádza, že *„Existujúce výskumné publikácie poukazujú na niektoré potenciálne zraniteľnosti, ktoré môžu existovať v modeloch umelej inteligencie a ktoré by mohli viesť k spracúvaniu osobných údajov,²² ako aj na spracúvanie osobných údajov, ku ktorému môže dochádzať pri nasadení modelov na použitie s inými údajmi, a to buď prostredníctvom aplikačných programovacích rozhraní („Application Programming Interfaces“ alebo „API“) alebo „výzvných“ rozhraní“²³.*
33. V rovnakom duchu je mimoriadne dynamický aj výskum v oblasti extrahovania tréningových údajov²⁴. Ukazuje, že v niektorých prípadoch je možné použiť prostriedky, ktoré s veľkou pravdepodobnosťou umožnia extrahovať osobné údaje z niektorých modelov umelej inteligencie, alebo jednoducho náhodne získať osobné údaje prostredníctvom interakcie s modelom umelej inteligencie (napríklad ako

²² Napríklad útoky založené na odvodzovaní členstva („Membership Inference Attacks“) ([OWASP](#)) a útoky založené na invertovaní modelu („Model Inversion Attacks“) ([OWASP](#) & [Veale a kol](#), 2018).

²³ Žiadosť, s. 1 – 2.

²⁴ V tejto súvislosti pozri napríklad: i) Veale M., Binns R., Edwards L., 2018, *Algorithms that remember: model inversion attacks and data protection law*. Phil. Trans. R. Soc. A 376: 20180083, available at <http://dx.doi.org/10.1098/rsta.2018.0083>; ii) Brown H., Lee K., Mirehghallah F., Shokri R., and Tramèr F., *What Does it Mean for a Language Model to Preserve Privacy?*, 2022, ACM Digital Library, FAccT '22, June 20, 2022, Seoul, Republic of Korea, available at <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*, January 2024, National Institute of Standards and Technology, available at <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*, arXiv:2012.07805v2 [cs.CR] 15 Jun 2021, available at <https://arxiv.org/pdf/2012.07805>; v) Fredrikson M., Jha S., Ristenpart T., *Model Inversion Attacks that Exploit Confidence Information and Basic Countermeasures*, ACM Digital Library, 12 October 2015, available at <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*, arXiv:1911.07135v2 [cs.LG] 18. 4. 2020, dostupné na <https://arxiv.org/pdf/1911.07135>.

súčasť systému umelej inteligencie). Nepretržité výskumné úsilie v tejto oblasti pomôže ďalej posúdiť zvyškové riziká regurgitácie²⁵ a extrakcie osobných údajov v každom danom prípade.

34. **Na základe uvedených úvah sa EDPB domnieva, že modely umelej inteligencie trénované na osobných údajoch nemožno vo všetkých prípadoch považovať za anonymné. Namiesto toho by sa určenie, či je model umelej inteligencie anonymný, malo posudzovať na základe konkrétnych kritérií od prípadu k prípadu.**

3.2 O okolnostiach, za ktorých by sa modely umelej inteligencie mohli považovať za anonymné a o súvisiacom preukázaní

35. Pokiaľ ide o prvú otázku žiadosti²⁶, od EDPB sa požaduje, aby objasnil okolnosti, za ktorých model umelej inteligencie, ktorý bol trénovaný s použitím osobných údajov, možno považovať za anonymný. Pokiaľ ide o otázku 1 písm. i) bod a) žiadosti²⁷, od EDPB sa požaduje, aby objasnil, ktoré dôkazy a/alebo dokumentáciu by mali dozorné orgány zohľadniť pri posudzovaní toho, či je model umelej inteligencie anonymný.

3.2.1 Všeobecné úvahy týkajúce sa anonymizácie v danom kontexte

36. Použitie výrazu „akékoľvek informácie“ vo vymedzení pojmu „osobné údaje“ v článku 4 ods. 1 všeobecného nariadenia o ochrane údajov odráža cieľ priznať tomuto pojmu široký rozsah, ktorý zahŕňa všetky druhy informácií za predpokladu, že „súvisia“ s dotknutou osobou, ktorá je identifikovaná alebo ju možno identifikovať priamo či nepriamo.
37. Informácie sa môžu vzťahovať na fyzickú osobu aj vtedy, keď sú technicky usporiadané alebo zakódované (napríklad len v strojovo čitateľnom formáte, či už proprietárnom alebo otvorenom) spôsobom, z ktorého nie je vzťah k tejto fyzickej osobe okamžite zrejmý. V takýchto prípadoch sa môžu softvérové aplikácie použiť na jednoduchú identifikáciu, rozpoznanie a extrakciu špecifických údajov. To platí najmä pre modely umelej inteligencie, ktorých parametre predstavujú štatistické vzťahy medzi trénovacími údajmi a kde môže byť možné extrahovať presné alebo nepresné (pretože štatisticky odvodené) osobné údaje, a to buď priamo zo vzťahov medzi údajmi zahrnutými v modeli, alebo dopytovaním tohto modelu.
38. Keďže modely umelej inteligencie zvyčajne neobsahujú záznamy, ktoré by mohli byť priamo izolované alebo prepojené, ale skôr parametre predstavujúce pravdepodobnostné vzťahy medzi údajmi obsiahnutými v modeli, v realistických scenároch môže byť možné z modelu odvodiť²⁸ informácie,

²⁵ V prípade systému umelej inteligencie založeného na generatívnej umelej inteligencii, regurgitácia zodpovedá situácii, keď by výstupy priamo súviseli s trénovacími údajmi.

²⁶ „Za akých okolností to môže nastať?“

²⁷ „Ak je to tak, ako možno preukázať kroky, ktoré sa prijali na zabezpečenie toho, aby model umelej inteligencie nespracúval osobné údaje?“

²⁸ (i) Carlini N., Chien S., Nasr M., Song S., Terzis A., Tramer F., *Membership Inference Attacks From First Principles*, arXiv:2112.03570, k dispozícii na <https://arxiv.org/abs/2112.03570>;

(ii) Crețu A.M., Guépin F., a De Montjoye Y.A., *Correlation inference attacks against machine learning models*. Sci. Adv.10, ead9260(2024). DOI:10.1126/sciadv.ad9260 k dispozícii na <https://www.science.org/doi/10.1126/sciadv.ad9260>;

(iii) Dana L., Pydi M. S., Chevalere Y., *Memorization in Attention-only Transformers* arXiv:2411.10115v1 [cs.AI] 15. novembra 2024, dostupné na: <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*. Künstl Intell, 13. júna 2024, dostupné na: <https://doi.org/10.1007/s13218-024-00851-y>;

napríklad zasahovanie do členstva. Preto, aby dozorný orgán mohol súhlasiť s prevádzkovateľom, že daný model umelej inteligencie možno považovať za anonymný, mal by prinajmenšom skontrolovať, či získal dostatočné dôkazy o tom, že s primeranými prostriedkami: i) osobné údaje súvisiace s tréningovými údajmi nie je možné extrahovať²⁹ z modelu a ii) akýkoľvek výstup vytvorený pri dopytovaní modelu sa nevzťahuje na dotknuté osoby, ktorých osobné údaje sa použili na tréningovanie modelu.

39. Dozorné orgány by pri posudzovaní toho, či sú tieto podmienky splnené, mali zvážiť tri prvky.
40. Po prvé, dozorné orgány by mali zvážiť prvky identifikované v najnovších stanoviskách pracovnej skupiny zriadenej podľa článku 29 a/alebo usmerneniach EDPB v tejto veci. Pokiaľ ide o anonymizáciu k dátumu tohto stanoviska, dozorné orgány by mali zvážiť prvky zahrnuté v stanovisku pracovnej skupiny zriadenej podľa článku 29 05/2014 o technikách anonymizácie („**stanovisko WP29 05/2014**“), v ktorom sa uvádza, že ak nie je možné vyčleniť, prepojiť a odvodiť informácie z údajne anonymného súboru údajov, údaje sa môžu považovať za anonymné³⁰. Uvádza sa v ňom tiež, že „*vždy, keď návrh nespĺňa jedno z uvedených kritérií, malo by sa vykonať dôkladné vyhodnotenie rizík identifikácie*“³¹. **Vzhľadom na uvedenú pravdepodobnosť extrakcie a odvodu sa EDPB domnieva, že modely umelej inteligencie si s veľkou pravdepodobnosťou budú vyžadovať takéto dôkladné vyhodnotenie rizík identifikácie.**
41. Po druhé, toto posúdenie by sa malo vykonať s prihliadnutím na „*všetky prostriedky, pri ktorých je primeraná pravdepodobnosť*“, že ich využije prevádzkovateľ alebo iná osoba“ na identifikáciu fyzických osôb³², pričom určenie týchto prostriedkov by sa malo zakladať na objektívnych faktoroch, ako sa vysvetľuje v odôvodnení 26 všeobecného nariadenia o ochrane údajov, ktoré môžu zahŕňať:
- a. charakteristiky samotných tréningových údajov, modelu umelej inteligencie a tréningového postupu³³;
 - b. kontext, v ktorom sa model umelej inteligencie zverejňuje a/alebo spracúva³⁴;

(v) Hu H., *Membership Inference Attacks and Defenses on Machine Learning Models Literature*, k dispozícii na: <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*, arXiv:2311.17035, 28. novembra 2023, k dispozícii na adrese: <https://arxiv.org/abs/2311.17035>;

(vii) Shokri R., Stronati M., Song C., Shmatikov V., *Membership Inference Attacks against Machine Learning Models* arXiv:1610.05820v2 [cs.CR], 31. marca 2017, dostupné na <https://arxiv.org/abs/1610.05820>;

(viii) Staab R., Vero M., Mislav Balunović, Martin Vechev, 2024, *Beyond Memorization: Violating Privacy Via Inference with Large Language Models*, arXiv:2310.07298v2, 6. mája 2024, dostupné na <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* arXiv:2406.02027v1 [cs.LG], 27. júna 2024, dostupné na <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* arXiv:2409.19798v1, [cs.LG], 29. september 2024, dostupné na <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*, arXiv:2308.15727v2 [cs.CL] 5, 5 novembra 2023, k dispozícii na: <https://arxiv.org/abs/2308.15727>.

²⁹ Extrakcia zahŕňa najmä prípad, keď sa osobné údaje odvodzujú zo samotného modelu umelej inteligencie, s malým alebo so žiadnym použitím vyhľadávacích rozhraní.

³⁰ Stanovisko WP29 05/2014, s. 24.

³¹ Stanovisko WP29 05/2014, s. 24.

³² Rozsudok SDEÚ z 19. októbra 2016, vec C-582/14, *Breyer/Bundesrepublik Deutschland* (ECLI:EU:C:2016:779), bod 43.

³³ Patria sem charakteristiky, ako je jedinečnosť záznamov v tréningových údajoch, presnosť informácií, agregácia, náhodnosť, a najmä to, ako tieto charakteristiky ovplyvňujú zraniteľnosť voči identifikácii.

³⁴ To zahŕňa kontextové prvky, ako je obmedzenie prístupu len na niektoré osoby a právne záruky.

- c. dodatočné informácie, ktoré by umožnili identifikáciu a ktoré môžu byť danej osobe prístupné;
 - d. náklady a množstvo času, ktoré by osoba potrebovala na získanie takýchto dodatočných informácií (v prípade, že ich ešte nemá k dispozícii)³⁵; a
 - e. dostupná technológia v čase spracúvania, ako aj technologický vývoj³⁶.
42. Po tretie, dozorné orgány by mali zvážiť, či prevádzkovatelia posúdili riziko identifikácie prevádzkovateľom a rôznymi typmi „iných osôb“ vrátane nezamýšľaných tretích strán prístupujúcich k modelu umelej inteligencie, pričom by mali zvážiť aj to, či ich možno odôvodnene považovať za schopné získať prístup k predmetným údajom alebo ich spracúvať.
43. **EDPB sa celkovo domnieva, že na to, aby sa model umelej inteligencie považoval za anonymný, by pri použití primeraných prostriedkov mala byť i) pravdepodobnosť priamej (vrátane pravdepodobnostnej) extrakcie osobných údajov týkajúcich sa osôb, ktorých osobné údaje sa použili na tréning modelu, ako aj ii) pravdepodobnosť úmyselného alebo neúmyselného získania takýchto osobných údajov z dopytov, nevýznamná³⁷ pre akúkoľvek dotknutú osobu. Dozorné orgány by štandardne mali vziať do úvahy, že modely umelej inteligencie si pravdepodobne budú vyžadovať dôkladné posúdenie pravdepodobnosti identifikácie, aby sa dospelo k záveru o ich možnej anonymnej povahe. Táto pravdepodobnosť by sa mala posudzovať s prihliadnutím na „všetky prostriedky, pri ktorých je primeraná pravdepodobnosť, že ich využije“ prevádzkovateľ alebo iná osoba, a mala by zohľadňovať aj neúmyselné (opätovné) použitie alebo zverejnenie modelu.**

3.2.2 Prvky na vyhodnotenie zvyškovej pravdepodobnosti identifikácie

44. Hoci sa opatrenia môžu prijímať vo fáze vývoja aj nasadzovania s cieľom znížiť pravdepodobnosť získania osobných údajov z modelu umelej inteligencie, pri hodnotení anonymity modelu umelej inteligencie by sa mal zvážiť aj priamy prístup k modelu.
45. Okrem toho by dozorné orgány mali v jednotlivých prípadoch posúdiť, či sú opatrenia zavedené prevádzkovateľom na zabezpečenie a preukázanie anonymity modelu umelej inteligencie primerané a účinné.
46. Záver posúdenia dozorného orgánu sa môže líšiť najmä medzi verejne dostupným modelom umelej inteligencie, ktorý je prístupný neznámemu počtu ľudí s neznámou škálou metód na extrakciu osobných údajov, a interným modelom umelej inteligencie prístupným len zamestnancom. Zatiaľ čo v oboch prípadoch by dozorné orgány mali overiť, či prevádzkovatelia splnili svoju povinnosť zodpovednosti podľa článku 5 ods. 2 a článku 24 všeobecného nariadenia o ochrane údajov, „*prostriedky, pri ktorých existuje primeraná pravdepodobnosť, že ich použijú*“ iné osoby, môžu mať vplyv na rozsah a povahu možných scenárov, ktoré sa majú zvážiť. Preto v závislosti od kontextu vývoja a nasadzovania modelu môžu dozorné orgány zvážiť rôzne úrovne testovania a odolnosti voči útokom.
47. V tejto súvislosti EDPB ďalej uvádza nenormatívny a neúplný zoznam možných prvkov, ktoré môžu dozorné orgány zohľadniť pri posudzovaní tvrdenia prevádzkovateľa o anonymite. Iné prístupy sú možné, ak poskytujú rovnocennú úroveň ochrany, najmä s prihliadnutím na súčasný stav techniky.
48. Prítomnosť alebo neprítomnosť ďalej uvedených prvkov nie je presvedčivým kritériom na posúdenie anonymity modelu umelej inteligencie.

³⁵ Rozsudok SDEÚ zo 7. marca 2024, vec C-479/22 P, OC/Európska komisia (ECLI:EU:C:2024:215), bod 50.

³⁶ Rozsudok SDEÚ zo 7. marca 2024, vec C-479/22 P, OC/Európska komisia (ECLI:EU:C:2024:215), bod 50.

³⁷ Rozsudok SDEÚ z 19. októbra 2016, vec C-582/14, Breyer/Bundesrepublik Deutschland (ECLI:EU:C:2016:779), bod 46 a rozsudok SDEÚ zo 7. marca 2024, vec C-479/22 P, OC/Európska komisia (ECLI:EU:C:2024:215), bod 51.

3.2.2.1 Návrh modelu umelej inteligencie

49. Pokiaľ ide o návrh modelu umelej inteligencie, dozorné orgány by mali vyhodnotiť prístupy prevádzkovateľov počas fázy vývoja. V tejto súvislosti by sa malo zväžiť uplatňovanie a účinnosť štyroch kľúčových oblastí (uvedených nižšie).

Výber zdrojov

50. Prvá oblasť hodnotenia zahŕňa preskúmanie výberu zdrojov používaných na trénovanie modelu umelej inteligencie. To zahŕňa hodnotenie zo strany dozorných orgánov všetkých prijatých opatrení s cieľom zabrániť získavaniu osobných údajov alebo ho obmedziť, okrem iného vrátane i) vhodnosti kritérií výberu; ii) relevantnosti a primeranosti vybraných zdrojov vzhľadom na zamýšľaný účel či účely a iii) toho, či boli vylúčené nevhodné zdroje.

Príprava a minimalizácia údajov

51. Druhá oblasť hodnotenia sa týka prípravy údajov pre fázu trénovania. Dozorné orgány by mali preskúmať najmä: i) či sa zvažilo použitie anonymných osobných údajov a/alebo osobných údajov, ktoré boli pseudonymizované, a ii) ak sa rozhodlo, že sa takéto opatrenia nepoužijú, dôvody tohto rozhodnutia s prihliadnutím na zamýšľaný účel; iii) stratégie a techniky minimalizácie údajov použité na obmedzenie objemu osobných údajov zahrnutých do procesu trénovania a iv) akékoľvek procesy filtrovania údajov zavedené pred trénovaním modelu s cieľom odstrániť irelevantné osobné údaje.

Metodické rozhodnutia týkajúce sa trénovania

52. Tretia oblasť hodnotenia sa týka výberu robustných metód pri vývoji modelu umelej inteligencie. Dozorné orgány by mali posúdiť metodické rozhodnutia, ktoré môžu výrazne znížiť alebo odstrániť identifikovateľnosť, okrem iného vrátane toho: i) či táto metodika využíva metódy regularizácie na zlepšenie zovšeobecnenia modelu a zníženie pretrénovania („overfitting“) a, čo je rozhodujúce, ii) či prevádzkovateľ zaviedol vhodné a účinné techniky na zachovanie súkromia (napr. diferenciálne súkromie).

Opatrenia týkajúce sa výstupov modelu

53. Posledná oblasť hodnotenia sa týka akýchkoľvek metód alebo opatrení pridaných do samotného modelu umelej inteligencie, ktoré nemusia mať vplyv na riziko priamej extrakcie osobných údajov pre daný model osobou, ktorá k nemu má priamy prístup, ale ktoré by mohli znížiť pravdepodobnosť získania osobných údajov týkajúcich sa trénovacích údajov z dopytov.

3.2.2.2 Analýza modelu umelej inteligencie

54. Aby dozorné orgány mohli posúdiť spoľahlivosť navrhnutého modelu umelej inteligencie, pokiaľ ide o anonymizáciu, prvým krokom je zabezpečiť, aby bol dizajn vyvinutý podľa plánu a podliehal účinnému inžinierskemu riadeniu. Dozorné orgány by mali posúdiť, či prevádzkovatelia vykonali nejaké audity (interné alebo externé) založené na dokumentoch, ktoré zahŕňajú hodnotenie vybraných opatrení a ich vplyvu na obmedzenie pravdepodobnosti identifikácie. Mohlo by to zahŕňať analýzu správ o preskúmaní kódu, ako aj teoretickú analýzu dokumentujúcu vhodnosť opatrení zvolených na zníženie pravdepodobnosti opätovnej identifikácie príslušného modelu.

3.2.2.3 Testovanie modelov umelej inteligencie a odolnosť voči útokom

55. Nakoniec by dozorné orgány mali zohľadniť rozsah, frekvenciu, množstvo a kvalitu testov, ktoré prevádzkovateľ na modeli vykonal. Dozorné orgány by mali zohľadniť najmä to, že úspešné testovanie, ktoré pokrýva všeobecne známe najmodernejšie útoky, môže byť len dôkazom odolnosti voči týmto útokom. Ku dňu vydania tohto stanoviska by to mohlo okrem iného zahŕňať štruktúrované testovanie proti: i) odvodzovaniu atribútov a zasahovaniu do členstva; ii) exfiltrácii; iii) regurgitácii trénovacích údajov; iv) inverzii modelu; alebo v) rekonštrukčným útokom.

3.2.2.4 Dokumentácia

56. V článkoch 5, 24, 25 a 30 všeobecného nariadenia o ochrane údajov a v prípadoch pravdepodobného vysokého rizika pre práva a slobody dotknutých osôb v článku 35 všeobecného nariadenia o ochrane údajov sa od prevádzkovateľov vyžaduje, aby primerane dokumentovali svoje spracovateľské operácie. To sa vzťahuje aj na akékoľvek spracúvanie, ktoré by zahŕňalo tréňovanie modelu umelej inteligencie, aj keď cieľom spracúvania je anonymizácia. Dozorné orgány by mali zvážiť takúto dokumentáciu a akékoľvek pravidelné posúdenie následných rizík pri spracúvaní vykonávanom prevádzkovateľmi, keďže ide o základné kroky na preukázanie toho, že osobné údaje sa nespracúvajú.
57. **EDPB sa domnieva, že dozorné orgány by mali zohľadniť dokumentáciu vždy, keď je potrebné vyhodnotiť tvrdenie o anonymite týkajúce sa daného modelu umelej inteligencie. EDPB poznamenáva, že ak dozorný orgán nie je schopný po posúdení tvrdenia o anonymite, a to aj vzhľadom na dokumentáciu, potvrdiť, že boli prijaté účinné opatrenia na anonymizáciu modelu umelej inteligencie, dozorný orgán by sa mohol domnievať, že prevádzkovateľ nesplnil svoje povinnosti týkajúce sa zodpovednosti podľa článku 5 ods. 2 všeobecného nariadenia o ochrane údajov. Preto by sa mal zvážiť aj súlad s inými ustanoveniami všeobecného nariadenia o ochrane údajov.**
58. V ideálnom prípade by dozorné orgány mali overiť, či dokumentácia prevádzkovateľa obsahuje:
- všetky informácie týkajúce sa posúdení vplyvu na ochranu údajov vrátane všetkých posúdení a rozhodnutí, v ktorých sa zistilo, že posúdenie vplyvu na ochranu údajov nie je potrebné;
 - akékoľvek poradenstvo alebo spätnú väzbu, ktoré poskytla **zodpovedná osoba** (v prípade, že zodpovedná osoba bola alebo mala byť vymenovaná);
 - informácie o technických a organizačných opatreniach prijatých pri navrhovaní modelu umelej inteligencie na zníženie pravdepodobnosti identifikácie vrátane modelu hrozby a posúdení rizika, na ktorých sú tieto opatrenia založené. Malo by to zahŕňať konkrétne opatrenia pre každý zdroj tréňovacích údajov vrátane príslušných zdrojových URL a opisov prijatých opatrení (alebo opatrení, ktoré už prijali poskytovatelia súborov údajov tretích strán);
 - technické a organizačné opatrenia prijaté vo všetkých fázach počas celého životného cyklu modelu, ktoré buď prispeli k nedostatku osobných údajov v modeli alebo ho potvrdili,
 - dokumentáciu preukazujúcu teoretickú odolnosť modelu umelej inteligencie voči technikám opätovnej identifikácie, ako aj kontrolné mechanizmy určené na obmedzenie alebo posúdenie úspešnosti a vplyvu hlavných útokov (regurgitácia, útoky založené na zasahovaní do členstva, exfiltrácia atď.). To môže zahŕňať najmä: i) pomer medzi množstvom tréňovacích údajov a počtom parametrov v modeli vrátane analýzy jeho vplyvu na model³⁸; ii) metriky pravdepodobnosti opätovnej identifikácie na základe súčasného stavu techniky; iii) správy o tom, ako bol model testovaný (kým, kedy, ako a v akom rozsahu) a iv) výsledky testov;

³⁸ Ricciato F., *A Cautionary Reflection on (Pseudo-)Synthetic Data from Deep Learning on Personal Data*, konferencia Privacy in Statistical Databases (PSD 2024), Antibes, Francúzsko, september 2024, prezentácie sú k dispozícii na adrese: https://cros.ec.europa.eu/system/files/2024-10/20240926_PSD2024_Ricciato_v6_1.pdf a Belkin M., Hsu D., Ma S., & Mandal S. (2019), *Reconciling modern machine-learning practice and the classical bias–variance trade-off*. Proceedings of the National Academy of Sciences, 24. júla 2019, 116(32) 15849-15854, dostupné na: <https://www.pnas.org/doi/10.1073/pnas.1903070116>

- f. dokumentáciu poskytnutú prevádzkovateľovi (prevádzkovateľom), ktorí model nasadzujú, a/alebo dotknutým osobám, najmä dokumentáciu týkajúcu sa opatrení prijatých na zníženie pravdepodobnosti identifikácie a pokiaľ ide o možné zvyškové riziká.

3.3 O vhodnosti oprávneného záujmu ako právneho základu pre spracúvanie osobných údajov v súvislosti s vývojom a nasadzovaním modelov umelej inteligencie

- 59. S cieľom odpovedať na druhú a tretiu otázku žiadosti EDPB najprv poskytne všeobecné pripomienky k niektorým dôležitým aspektom, ktoré by dozorné orgány mali zohľadniť bez ohľadu na právny základ spracúvania pri posudzovaní toho, ako môžu prevádzkovatelia preukázať súlad so všeobecným nariadením o ochrane údajov v kontexte modelov umelej inteligencie. EDPB, vychádzajúc z Usmernení 1/2024 k spracúvaniu osobných údajov na základe článku 6 ods. 1 písm. f) všeobecného nariadenia o ochrane údajov³⁹, potom zváži tri kroky, ktoré si vyžaduje posúdenie oprávneného záujmu v kontexte vývoja a nasadzovania modelov umelej inteligencie.

3.3.1 Všeobecné poznámky

- 60. EDPB pripomína, že vo všeobecnom nariadení o ochrane údajov sa nestanovuje žiadna hierarchia medzi rôznymi právnymi základmi stanovenými v článku 6 ods. 1 všeobecného nariadenia o ochrane údajov⁴⁰.
- 61. V článku 5 všeobecného nariadenia o ochrane údajov sa stanovujú zásady týkajúce sa spracúvania osobných údajov. EDPB zdôrazňuje tie, ktoré sú dôležité pre toto stanovisko, a dozorné orgány by ich mali aspoň zohľadniť pri posudzovaní konkrétnych modelov umelej inteligencie, ako aj najrelevantnejších požiadaviek z iných ustanovení všeobecného nariadenia o ochrane údajov, pričom sa zohľadní rozsah pôsobnosti tohto stanoviska.
- 62. **Zásada zodpovednosti** (článok 5 ods. 2 všeobecného nariadenia o ochrane údajov) – v tejto zásade sa stanovuje, že prevádzkovateľ je zodpovedný za súlad so všeobecným nariadením o ochrane údajov a musí byť schopný tento súlad preukázať. V tomto ohľade by sa úlohy a zodpovednosti strán, ktoré spracúvajú osobné údaje v súvislosti s vývojom alebo nasadzovaním modelu umelej inteligencie, mali posúdiť pred uskutočnením spracúvania, aby sa od začiatku vymedzili povinnosti prevádzkovateľov alebo spoločných prevádzkovateľov a prípadných sprostredkovateľov.
- 63. **Zásady zákonnosti, spravodlivosti a transparentnosti** (článok 5 ods. 1 písm. a) všeobecného nariadenia o ochrane údajov) – pri posudzovaní zákonnosti spracúvania v kontexte modelov umelej inteligencie považuje EDPB vzhľadom na článok 6 ods. 1 všeobecného nariadenia o ochrane údajov za užitočné rozlišovať rôzne fázy spracúvania osobných údajov⁴¹. Zásada spravodlivosti, ktorá úzko súvisí so zásadou transparentnosti, si vyžaduje, aby osobné údaje neboli spracúvané nespravodlivými metódami alebo podvodným konaním, alebo spôsobom, ktorý je „pre dotknutú osobu neodôvodnene škodlivý, nezákonne diskriminačný, neočakávaný alebo zavádzajúci“⁴². Vzhľadom na zložitosť príslušných technológií by sa preto informácie o spracúvaní osobných údajov v rámci modelov umelej

³⁹ Pozri usmernenia EDPB 1/2024 k spracúvaniu osobných údajov na základe článku 6 ods. 1 písm. f) všeobecného nariadenia o ochrane údajov, verzia 1.0, prijaté 8. októbra 2024.

⁴⁰ Tamže, bod 1.

⁴¹ Správa EDPB o práci, ktorú vykonala pracovná skupina pre ChatGPT, prijatá 23. mája 2024, bod 14.

⁴² Správa EDPB o práci, ktorú vykonala pracovná skupina pre ChatGPT, prijatá 23. mája 2024, bod 23; usmernenia EDPB 4/2019 o špecificky navrhutej a štandardnej ochrane údajov, verzia 2.0, prijaté 20. októbra 2020, bod 69; usmernenia pracovnej skupiny zriadenej podľa článku 29 o transparentnosti podľa nariadenia 2016/679, revidované a prijaté 11. apríla 2018, schválené Európskym výborom pre ochranu údajov 25. mája 2018, odsek 2.

inteligencie mali poskytovať prístupným, zrozumiteľným a používateľsky ústretovým spôsobom⁴³. Transparentnosť spracúvania osobných údajov zahŕňa najmä dodržiavanie informačných povinností stanovených v článkoch 12 až 14 všeobecného nariadenia o ochrane údajov⁴⁴, ktoré si v prípade automatizovaného rozhodovania vrátane profilovania takisto vyžadujú zmysluplné informácie o použitej logike, ako aj význame a predpokladaných dôsledkoch spracúvania pre dotknutú osobu⁴⁵. Vzhľadom na to, že vývojové fázy modelov umelej inteligencie môžu zahŕňať získavanie veľkého množstva údajov z verejne prístupných zdrojov (napríklad prostredníctvom techník extrahovania údajov z webu), spoliehanie sa na výnimku stanovenú v článku 14 ods. 5 písm. b) všeobecného nariadenia o ochrane údajov je prísne obmedzené na prípady, keď sú požiadavky tohto ustanovenia úplne splnené⁴⁶.

64. **Zásady obmedzenia účelu a minimalizácie údajov** (článok 5 ods. 1 písm. b), c) všeobecného nariadenia o ochrane údajov) – V súlade so zásadou minimalizácie údajov si vývoj a nasadzovanie modelov umelej inteligencie vyžaduje, aby osobné údaje boli primerané, relevantné a nevyhnutné vzhľadom na účel. To môže zahŕňať spracúvanie osobných údajov s cieľom zabrániť riziku možných skreslení a chýb, ak je to jasne a konkrétne identifikované v rámci účelu, a osobné údaje sú nevyhnutné na tento účel (napríklad nie je možné ich účinne dosiahnuť spracúvaním iných údajov vrátane syntetických alebo anonymizovaných údajov)⁴⁷. Pracovná skupina zriadená podľa článku 29 už zdôraznila, že „*účel získavania údajov musí byť jasne a konkrétne určený [...]*“⁴⁸. Pri posudzovaní, či je sledovaný účel legitímny, konkrétny a výslovný a či je spracúvanie v súlade so zásadou minimalizácie údajov, by sa mala najprv identifikovať príslušná spracovateľská činnosť. Konkrétne, rôzne etapy vo fázach vývoja alebo nasadzovania môžu predstavovať rovnaké alebo odlišné spracovateľské činnosti a môžu zahŕňať po sebe nasledujúcich prevádzkovateľov alebo spoločných prevádzkovateľov. V niektorých prípadoch je možné určiť účel, ktorý sa bude sledovať počas nasadzovania modelu umelej inteligencie v počiatočnej fáze vývoja. Aj v opačnom prípade by už mal byť jasný určitý kontext tohto nasadzovania, a preto by sa malo zväziť, ako tento kontext ovplyvňuje účel vývoja. Pri preskúmaní účelu spracúvania v danej fáze vývoja by dozorné orgány mali od prevádzkovateľa (prevádzkovateľov) očakávať určitý stupeň podrobnosti a vysvetlenie toho, ako tieto podrobnosti vplyvajú na účel spracúvania. To môže zahŕňať napríklad informácie o type vyvinutého modelu umelej inteligencie, jeho očakávaných funkciách a akomkoľvek inom relevantnom kontexte, ktorý je už v tejto fáze známy. Kontext nasadzovania by mohol zahŕňať napríklad aj to, či sa model vyvíja na interné nasadenie, či prevádzkovateľ plánuje predávať alebo distribuovať model tretím stranám po jeho vývoji vrátane toho, či je model primárne určený na použitie na výskumné alebo komerčné účely.
65. **Práva dotknutých osôb** (kapitola III všeobecného nariadenia o ochrane údajov) – bez ohľadu na potrebu dozorných orgánov zabezpečiť, aby sa pri vývoji a nasadzovaní modelov umelej inteligencie

⁴³ Usmernenia pracovnej skupiny zriadenej podľa článku 29 o transparentnosti podľa nariadenia 2016/679, revidované a prijaté 11. apríla 2018, schválené Európskym výborom pre ochranu údajov 25. mája 2018, ods. 5.

⁴⁴ Pozri tiež odôvodnenie 39 všeobecného nariadenia o ochrane údajov, v ktorom sa uvádza, že „*Pre fyzické osoby by malo byť transparentné, že sa získavajú, používajú, konzultujú alebo inak spracúvajú osobné údaje, ktoré sa ich týkajú, ako aj to, v akom rozsahu sa tieto osobné údaje spracúvajú alebo budú spracúvať (...)*“.

⁴⁵ Článok 13 ods. 2 písm. f) všeobecného nariadenia o ochrane údajov a článok 14 ods. 2 písm. g) všeobecného nariadenia o ochrane údajov.

⁴⁶ Správa EDPB o práci, ktorú vykonala pracovná skupina pre ChatGPT, prijatá 23. mája 2024, bod 27.

⁴⁷ Okrem toho sa v článku 10 ods. 5 aktu o umelej inteligencii stanovujú osobitné pravidlá spracúvania osobitných kategórií osobných údajov v súvislosti s vysokorizikovými systémami umelej inteligencie na účely zabezpečenia odhaľovania a nápravy zaujatosti.

⁴⁸ Stanovisko č. 03/2013 pracovnej skupiny zriadenej podľa článku 29 o obmedzení účelu (WP203), s. 15 – 16.

prevádzkovateľmi dodržiavali všetky práva dotknutých osôb, EDPB pripomína, že vždy, keď sa prevádzkovateľ spolieha na oprávnený záujem ako právny základ, uplatňuje sa a malo by sa zabezpečiť právo namietať podľa článku 21 všeobecného nariadenia o ochrane údajov⁴⁹.

3.3.2 Úvahy o troch krokoch posudzovania oprávneného záujmu v kontexte vývoja a nasadzovania modelov umelej inteligencie

66. S cieľom určiť, či dané spracúvanie osobných údajov môže byť založené na článku 6 ods. 1 písm. f) všeobecného nariadenia o ochrane údajov, by dozorné orgány mali overiť, či prevádzkovatelia dôkladne posúdili a zdokumentovali, či sú splnené tieto tri kumulatívne podmienky: i) sledovanie oprávneného záujmu prevádzkovateľom alebo treťou stranou; ii) spracúvanie je nevyhnutné na sledovanie oprávneného záujmu a iii) nad oprávneným záujmom neprevyšujú záujmy alebo základné práva a slobody dotknutých osôb⁵⁰.

3.3.2.1 Prvý krok – Sledovanie oprávneného záujmu prevádzkovateľom alebo treťou stranou

67. Záujem je širší záujem alebo prospech, ktorý môže mať prevádzkovateľ alebo tretia strana pri vykonávaní konkrétnej spracovateľskej činnosti⁵¹. Zatiaľ čo všeobecné nariadenie o ochrane údajov a SDEÚ uznali, že viaceré záujmy sú oprávnené⁵², posúdenie oprávnenosti daného záujmu by malo byť výsledkom analýzy jednotlivých prípadov.
68. Ako pripomína EDPB vo svojich usmerneniach o oprávnenom záujme⁵³, záujem možno považovať za oprávnený, ak sú splnené tieto tri kumulatívne kritériá:

- a. Záujem je zákonný⁵⁴;

⁴⁹ Podľa článku 21 všeobecného nariadenia o ochrane údajov, ak dotknutá osoba namieta z dôvodov týkajúcich sa jej konkrétnej situácie proti spracúvaniu osobných údajov, ktoré sa jej týkajú, prevádzkovateľ nesmie ďalej spracúvať osobné údaje, pokiaľ nepreukáže nevyhnutné oprávnené dôvody na spracúvanie, ktoré prevažujú nad záujmami, právami a slobodami dotknutej osoby, alebo dôvody na preukazovanie, uplatňovanie alebo obhajovanie právnych nárokov. Preto musia dozorné orgány zohľadniť dva aspekty: či je prevádzkovateľ schopný preukázať takéto presvedčivé prevažujúce oprávnené dôvody a či je možné uplatniť právo namietať.

⁵⁰ Rozsudok SDEÚ zo 4. júla 2023, vec C-252/21, *Meta v. Bundeskartellamt* (ECLI:EU:C:2023:537), ods. 106; rozsudok SDEÚ z 11. decembra 2019, C-708/18, *Asociația de Proprietari bloc M5A-ScaraA* (ECLI:EU:C:2019:1064), bod 40. Pozri aj usmernenia EDPB 1/2024 o spracúvaní osobných údajov na základe článku 6 ods. 1 písm. f) všeobecného nariadenia o ochrane údajov, verzia 1.0 prijatá 8. októbra 2024, bod 12 a nasl. Ako sa pripomína v týchto usmerneniach, toto „posúdenie by sa malo vykonať na začiatku spracúvania so zapojením zodpovednej osoby (ak je určená) a prevádzkovateľ by ho mal zdokumentovať v súlade so zásadou zodpovednosti stanovenou v článku 5 ods. 2 všeobecného nariadenia o ochrane údajov“.

⁵¹ Usmernenia EDPB 1/2024 o spracúvaní osobných údajov na základe článku 6 ods. 1 písm. f) všeobecného nariadenia o ochrane údajov, verzia 1.0, prijaté 8. októbra 2024, bod 14.

⁵² Usmernenia EDPB 1/2024 o spracúvaní osobných údajov na základe článku 6 ods. 1 písm. f) všeobecného nariadenia o ochrane údajov, verzia 1.0, prijaté 8. októbra 2024, bod 16.

⁵³ Usmernenia EDPB 1/2024 o spracúvaní osobných údajov na základe článku 6 ods. 1 písm. f) všeobecného nariadenia o ochrane údajov, verzia 1.0, prijaté 8. októbra 2024, bod 17.

⁵⁴ Rozsudok Súdneho dvora zo 4. októbra 2024, vec C-621/22, *Koninklijke Nederlandse Lawn Tennisbond* (ECLI:EU:C:2024:857), bod 49, v ktorom Súdny dvor zdôraznil, že oprávnený záujem nemôže byť v rozpore so zákonom. V tejto súvislosti EDPB zdôrazňuje, že pri posudzovaní zákonnosti daného záujmu by sa prípadne mali zohľadniť legislatívne rámce. Pozri napríklad: Článok 26 ods. 3 a článok 28 nariadenia Európskeho parlamentu a Rady (EÚ) 2022/2065 z 19. októbra 2022 o jednotnom trhu s digitálnymi službami a o zmene smernice 2000/31/ES (akt o digitálnych službách) o zakázanej cielenej reklame pre maloleté osoby; článok 5 ods. 1 a 2 aktu o umelej inteligencii o zakázaných praktikách umelej inteligencie (manipulatívne praktiky a pod prahovou hodnotou vedomia); spracúvanie v rozpore s právami duševného vlastníctva a ustanoveniami smernice (EÚ) 2019/790 o autorskom práve a právach súvisiacich s autorským právom na digitálnom jednotnom trhu.

- b. Záujem je jasne a presne vyjadrený; a
- c. Záujem je skutočný a prítomný, nie špekulatívny.

69. S výhradou ďalších dvoch krokov vyžadovaných pri posudzovaní oprávneného záujmu môžu v súvislosti s modelmi umelej inteligencie predstavovať oprávnený záujem tieto príklady: i) vývoj služby konverzačného agenta na pomoc používateľom; ii) vývoj systému umelej inteligencie na odhaľovanie podvodného obsahu alebo správania a iii) zlepšenie odhaľovania hrozieb v informačnom systéme.

3.3.2.2 Druhý krok – Analýza nevyhnutnosti spracúvania na účely oprávneného záujmu

70. Druhý krok posúdenia spočíva v určení toho, či je spracúvanie osobných údajov nevyhnutné na účely sledovaného oprávneného záujmu/sledovaných záujmov⁵⁵ (tzv. test nevyhnutnosti).
71. V odôvodnení 39 všeobecného nariadenia o ochrane údajov sa stanovuje, že „Osobné údaje by sa mali spracúvať len vtedy, ak účel spracúvania nebolo možné za primeraných podmienok dosiahnuť inými prostriedkami“. Podľa SDEÚ a predchádzajúcich usmernení EDPB by sa podmienka týkajúca sa nevyhnutnosti spracúvania mala preskúmať vzhľadom na základné práva a slobody dotknutých osôb a v spojení so zásadou minimalizácie údajov zakotvenou v článku 5 ods. 1 písm. c) všeobecného nariadenia o ochrane údajov⁵⁶.
72. Metodika, na ktorú sa odvoláva SDEÚ, zohľadňuje kontext spracúvania, ako aj účinky na prevádzkovateľa a dotknuté osoby. Posúdenie nevyhnutnosti preto zahŕňa dva prvky: i) či spracovateľská činnosť umožní dosiahnutie účelu⁵⁷; a ii) či neexistuje menej rušivý spôsob dosiahnutia tohto účelu⁵⁸.

Usmernenia⁵⁵ EDPB 1/2024 k spracúvaniu osobných údajov na základe článku 6 ods. 1 písm. f) všeobecného nariadenia o ochrane údajov, verzia 1.0, prijaté 8. októbra 2024, body 28 až 30.

⁵⁶ Rozsudok Súdneho dvora Európskej únie zo 4. júla 2023, vec C-252/21, *Meta/Bundeskartellamt* (ECLI:EU:C:2023:537), body 108 a 109, s odkazom aj na Súdny dvor Európskej únie, rozsudok z 11. decembra 2019, vec C-708/18, *Asociația de Proprietari bloc M5A-Scara A* (ECLI:EU:C:2019:1064), bod 48; rozsudok SDEÚ z 9. novembra 2010, spojené veci C-92/09 a C-93/09, *Volker und Markus Schecke* (ECLI:EU:C:2010:662), body 85 a 86; rozsudok Súdneho dvora z 22. júna 2021, vec C-439/19, *Latvijas Republikas Saeima* (ECLI:EU:C:2021:504), body 98, 109, 110, 113. Pozri tiež napríklad: Usmernenia EDPB 3/2019 k spracúvaniu osobných údajov prostredníctvom kamerových zariadení, verzia 2.0, prijaté 29. januára 2020, body 24 – 26 a 73; usmernenia EDPB 2/2019 k spracúvaniu osobných údajov podľa článku 6 ods. 1 písm. b) všeobecného nariadenia o ochrane údajov v súvislosti s poskytovaním služieb online dotknutým osobám, verzia 2.0, prijaté 8. októbra 2019, body 23 – 25; stanovisko EDPB 11/2024 k používaniu rozpoznávania tváre na zjednodušenie toku cestujúcich na letisku, verzia 1.1, prijaté 23. mája 2024, bod 27.

⁵⁷ Pozri SDEÚ, rozsudok zo 16. decembra 2008, vec C-524/06, *Heinz Huber/Bundesrepublik Deutschland* (ECLI:EU:C:2008:724), bod 66. V tej istej veci pozri aj stanovisko generálneho advokáta Poiaresa Madura vo veci C-524/06, *Heinz Huber proti Bundesrepublik Deutschland* (ECLI:EU:C:2008:194), bod 16, v ktorom sa uvádza „vhodným kritériom na tomto mieste je kritérium efektivity a záleží na vnútroštátnych súdoch, aby ho uplatnili. Otázka, ktorú si musia položiť, spočíva v tom, či existujú iné spôsoby spracúvania údajov, ktorými môžu prístahovateľské orgány uplatňovať pravidlá pobytového statusu. Ak bude odpoveď na túto otázku kladná, musí sa centralizované uchovávanie a spracúvanie údajov občanov Únie považovať za protiprávne. Nie je nevyhnutné, aby alternatívny systém bol najefektívnejší alebo najvhodnejší; stačí, ak bude schopný fungovať dostatočne. Inými slovami, aj keď je centrálny register pre používateľov efektívnejší, vhodnejší alebo jednoduchší ako jeho alternatívy (akými sú decentralizované, miestne registre), posledné uvedené systémy majú byť jasne uprednostňované, pokiaľ ich možno použiť na určenie pobytového statusu občanov Spoločenstva.

⁵⁸ Pozri SDEÚ, rozsudok z 27. septembra 2017, vec C-73/16, *Peter Puškár* (ECLI:EU:C:2017:725), bod 113: „Je tak úlohou vnútroštátneho súdu overiť, či vytvorenie sporného zoznamu a zápis mien dotknutých osôb do tohto zoznamu sú spôsobilé uskutočniť nimi sledované ciele a či neexistujú iné menej obmedzujúce prostriedky na dosiahnutie týchto cieľov“; Pozri napríklad aj stanovisko generálneho advokáta Rantosa vo veci C-252/21, *Meta*

73. Napríklad, podľa okolností, zamýšľaný objem osobných údajov zahrnutých do modelu umelej inteligencie sa musí posúdiť vzhľadom na menej rušivé alternatívy, ktoré môžu byť primerane dostupné, aby sa rovnako účinne dosiahol účel sledovaného oprávneného záujmu. Ak je dosiahnutie účelu možné aj prostredníctvom modelu umelej inteligencie, ktorý nevyžaduje spracúvanie osobných údajov, spracúvanie osobných údajov by sa malo považovať za nepotrebné. Toto je obzvlášť dôležité pre vývoj modelov umelej inteligencie. Pri posudzovaní, či je splnená podmienka nevyhnutnosti, by orgány dohľadu mali venovať osobitnú pozornosť množstvu spracúvaných osobných údajov a tomu, či je to primerané na sledovanie príslušného oprávneného záujmu, a to aj vzhľadom na zásadu minimalizácie údajov.
74. Pri posudzovaní nevyhnutnosti by sa mal zohľadniť aj širší kontext zamýšľaného spracúvania osobných údajov. Existencia prostriedkov, ktoré menej zasahujú do základných práv a slobôd dotknutých osôb, sa môže líšiť v závislosti od toho, či má prevádzkovateľ priamy vzťah s dotknutými osobami (údaje prvej strany) alebo nie (údaje tretej strany). SDEÚ poskytol niekoľko úvah, ktoré treba zohľadniť pri analýze nevyhnutnosti spracúvania údajov prvej strany na účely sledovaného oprávneného záujmu (sledovaných oprávnených záujmov) (aj keď v súvislosti so sprístupnením takýchto údajov tretím stranám)⁵⁹.
75. K splneniu testu nevyhnutnosti môže prispieť aj zavedenie technických záruk na ochranu osobných údajov. To by mohlo zahŕňať napríklad vykonávacie opatrenia, ako sú opatrenia uvedené v oddiele 3.2.2, a to takým spôsobom, že sa nedosiahne anonymizácia, čo však stále znižuje jednoduchosť identifikácie dotknutých osôb. EDPB poznamenáva, že niektoré z týchto opatrení, ak sa nevyžadujú na dosiahnutie súladu so všeobecným nariadením o ochrane údajov, môžu predstavovať dodatočné záruky, ako sa ďalej analyzuje v pododdieli „zmierňujúce opatrenia“ v rámci oddielu 3.3.2.3⁶⁰.

3.3.2.3 Tretí krok – test vyváženia

76. Tretím krokom posúdenia oprávneného záujmu je „**vyvažovanie**“ (v tomto dokumente označované aj ako „**test vyváženia**“)⁶¹. Tento krok spočíva v identifikácii a opise rôznych protichodných práv a záujmov, o ktoré ide⁶², t. j. na jednej strane záujmov, základných práv a slobôd dotknutých osôb a na druhej strane záujmov prevádzkovateľa alebo tretej strany. Potom by sa mali zvážiť konkrétne okolnosti prípadu, aby sa preukázalo, že oprávnený záujem je vhodným právnym základom pre príslušné spracovateľské činnosti⁶³.

Záujmy, základné práva a slobody dotknutých osôb

77. V článku 6 ods. 1 písm. f) všeobecného nariadenia o ochrane údajov sa stanovuje, že pri posudzovaní rôznych zložiek v kontexte testu vyváženia by mal prevádzkovateľ zohľadniť záujmy, základné práva

v. *Bundeskartellamt*, ECLI:EU:C:2022:704, bod 61, v ktorom sa uvádza „[...] Musí preto existovať úzka súvislosť medzi spracúvaním a sledovaným cieľom bez toho, aby existovali alternatívne riešenia, ktoré by v širšej miere rešpektovali ochranu osobných údajov, pretože nestačí, aby bolo spracúvanie údajov založené len na jeho užitočnosti pre prevádzkovateľa“.

⁵⁹ SDEÚ, rozsudok zo 4. októbra 2024, vec C-621/22, *Koninklijke Nederlandse Lawn Tennisbond* (ECLI:EU:C:2024:857), body 51 – 53.

⁶⁰ Pozri usmernenia EDPB 1/2024 k spracúvaniu osobných údajov na základe článku 6 ods. 1 písm. f) všeobecného nariadenia o ochrane údajov, verzia 1.0, prijaté 8. októbra 2024, bod 57.

⁶¹ Pozri usmernenia EDPB 1/2024 k spracúvaniu osobných údajov na základe článku 6 ods. 1 písm. f) všeobecného nariadenia o ochrane údajov, verzia 1.0, prijaté 8. októbra 2024, body 31 až 60.

⁶² Pozri usmernenia EDPB 1/2024 k spracúvaniu osobných údajov na základe článku 6 ods. 1 písm. f) všeobecného nariadenia o ochrane údajov, verzia 1.0, prijaté 8. októbra 2024, bod 32.

⁶³ Pozri usmernenia EDPB 1/2024 k spracúvaniu osobných údajov na základe článku 6 ods. 1 písm. f) GDPR, verzia 1.0, prijaté 8. októbra 2024, bod 32, tiež s odkazom na rozsudok SDEÚ zo 4. júla 2023, vec C-252/21, *Meta v. Bundeskartellamt* (ECLI:EU:C:2023:537), bod 110.

a slobody dotknutých osôb. Záujmy dotknutých osôb sú tie, ktoré môžu byť príslušným spracúvaním ovplyvnené. V kontexte fázy vývoja modelu umelej inteligencie môžu tieto záujmy zahŕňať okrem iného záujem o sebaurčenie a zachovanie kontroly nad vlastnými osobnými údajmi (napr. údajmi zhromaždenými na účely vývoja modelu). V súvislosti s nasadením modelu umelej inteligencie môžu záujmy dotknutých osôb okrem iného zahŕňať záujmy pri zachovaní kontroly nad vlastnými osobnými údajmi (napr. údaje spracúvané po nasadení modelu), finančné záujmy (napr. ak model umelej inteligencie používa dotknutá osoba na generovanie príjmov alebo ho používa jednotlivec v kontexte svojej profesionálnej činnosti), osobné výhody (napr. ak sa model umelej inteligencie používa na zlepšenie dostupnosti určitých služieb) alebo sociálno-ekonomické záujmy (napr. ak model umelej inteligencie umožňuje prístup k lepšej zdravotnej starostlivosti alebo uľahčuje uplatňovanie základného práva, ako je prístup k vzdelávaniu)⁶⁴.

78. Čím presnejšie je záujem vymedzený vzhľadom na zamýšľaný účel spracúvania, tým lepšie umožní jasne pochopiť realitu prínosov a rizík, ktoré sa majú zohľadniť v rámci testu vyváženia.
79. V súvislosti so základnými právami a slobodami dotknutých osôb môže vývoj a nasadzovanie modelov umelej inteligencie predstavovať vážne riziko pre práva chránené Chartou základných práv EÚ (ďalej len „**Charta EÚ**“), okrem iného vrátane práva na súkromný a rodinný život (článok 7 Charty EÚ) a práva na ochranu osobných údajov (článok 8 Charty EÚ). Tieto riziká sa môžu vyskytnúť vo fáze vývoja, napríklad ak sa osobné údaje extrahujú proti želaniu dotknutých osôb alebo bez ich vedomia. Tieto riziká sa môžu vyskytnúť aj vo fáze nasadzovania, napríklad ak sa osobné údaje spracúvajú modelom (alebo ako jeho súčasť) spôsobom, ktorý je v rozpore s právami dotknutých osôb, alebo ak je možné náhodne alebo prostredníctvom útokov (napr. zasahovanie do členstva, extrakcia alebo invertovanie modelu) odvodiť, aké osobné údaje sa nachádzajú v učiacej sa databáze. Takéto situácie predstavujú riziko pre súkromie dotknutých osôb, ktorých údaje sa môžu objaviť vo fáze nasadzovania systému umelej inteligencie (napr. riziko poškodenia dobrého mena, krádeže totožnosti alebo podvodu, bezpečnostné riziko v závislosti od povahy údajov).
80. V závislosti od konkrétneho prípadu môžu byť ohrozené aj iné základné práva. Napríklad rozsiahle a nediferencované získavanie údajov modelmi umelej inteligencie vo fáze vývoja môže vytvoriť pocit sledovania pre dotknuté osoby, najmä vzhľadom na ťažkosti s predchádzaním extrahovaniu verejných údajov. To môže viesť jednotlivcov k autocenzúre a predstavovať riziko narušenia ich slobody prejavu (článok 11 Charty EÚ). Vo fáze nasadzovania sú riziká pre slobodu prejavu prítomné aj vtedy, keď sa modely umelej inteligencie používajú na blokovanie zverejňovania obsahu zo strany dotknutých osôb. Okrem toho model umelej inteligencie, ktorý odporúča nevhodný obsah pre zraniteľné osoby, môže predstavovať riziko pre ich duševné zdravie (článok 3 ods. 1 Charty EÚ). V iných prípadoch môže nasadenie modelov umelej inteligencie viesť aj k nepriaznivým dôsledkom na právo jednotlivca na vykonávanie povolania (článok 15 Charty EÚ), napríklad keď sa žiadosti o zamestnanie predbežne vyberajú pomocou modelu umelej inteligencie. Rovnako by model umelej inteligencie mohol predstavovať riziko pre právo na nediskrimináciu (článok 21 Charty EÚ), ak by diskriminoval jednotlivcov na základe určitých osobných charakteristík (napríklad štátnej príslušnosti alebo pohlavia). Okrem toho môže nasadzovanie modelov umelej inteligencie predstavovať aj riziká pre bezpečnosť a ochranu jednotlivca (napr. ak sa model umelej inteligencie používa so zlým úmyslom), ako aj riziká pre jeho fyzickú a duševnú nedotknuteľnosť⁶⁵.

⁶⁴ Pozri usmernenia EDPB 1/2024 k spracúvaniu osobných údajov na základe článku 6 ods. 1 písm. f) všeobecného nariadenia o ochrane údajov, verzia 1.0, prijaté 8. októbra 2024, bod 38.

⁶⁵ Usmernenia 1/2024 k spracúvaniu osobných údajov na základe článku 6 ods. 1 písm. f) všeobecného nariadenia o ochrane údajov, verzia 1.0, prijaté 8. októbra 2024, bod 46.

81. Nasadzovanie modelov umelej inteligencie môže mať takisto pozitívny vplyv na určité základné práva, napr. model môže podporovať právo na duševnú nedotknuteľnosť osoby (článok 3 charty), napríklad ak sa model umelej inteligencie používa na identifikáciu škodlivého obsahu online; alebo model môže uľahčiť prístup k určitým základným službám alebo uľahčiť výkon základných práv, ako je prístup k informáciám (článok 11 Charty EÚ) alebo prístup k vzdelávaniu (článok 14 charty EÚ).

Vplyv spracúvania na dotknuté osoby

82. Spracúvanie osobných údajov, ktoré sa uskutočňuje počas vývoja a nasadzovania modelov umelej inteligencie, môže mať vplyv na dotknuté osoby rôznymi spôsobmi, ktoré môžu byť pozitívne alebo negatívne⁶⁶. Ak napríklad spracovateľská činnosť prináša dotknutej osobe výhody, možno ich zohľadniť v rámci testu vyváženosti. Hoci existencia takýchto výhod môže viesť dozorný orgán k záveru, že záujmy, základné práva a slobody dotknutých osôb neprevyšujú nad záujmami prevádzkovateľa alebo tretej strany, takýto záver môže byť len výsledkom analýzy jednotlivých prípadov, pričom sa zohľadnia všetky príslušné faktory.
83. Vplyv spracúvania na dotknuté osoby môže byť ovplyvnený i) povahou údajov spracúvaných modelmi; ii) kontextom spracúvania a iii) ďalšími dôsledkami, ktoré môže spracúvanie mať⁶⁷.
84. V súvislosti s **povahou spracúvaných údajov** treba pripomenúť, že – okrem osobitných kategórií osobných údajov a údajov týkajúcich sa uznania viny za trestné činy a priestupky, ktoré požívajú dodatočnú ochranu podľa článkov 9 a 10 všeobecného nariadenia o ochrane údajov – môže spracúvanie niektorých iných kategórií osobných údajov viesť k významným dôsledkom pre dotknuté osoby. V tejto súvislosti by sa spracúvanie určitých druhov osobných údajov, ktoré odhaľujú vysoko súkromné informácie (napr. finančné údaje alebo lokalizačné údaje) na účely vývoja a nasadzovania modelu umelej inteligencie, malo považovať za spracúvanie s možným závažným vplyvom na dotknuté osoby. Vo fáze nasadzovania môžu mať dôsledky takéhoto spracúvania údajov pre dotknuté osoby napríklad ekonomický charakter (napr. diskriminácia v súvislosti so zamestnaním) a/alebo vplyv na dobrú povesť (napr. ohováranie).
85. V súvislosti s **kontextom spracúvania** je potrebné najprv identifikovať prvky, ktoré by mohli predstavovať riziko pre dotknuté osoby (napr. spôsob, akým bol model vyvinutý, spôsob, akým môže byť model nasadený, a/alebo či sú bezpečnostné opatrenia použité na ochranu osobných údajov primerané). Povaha modelu a zamýšľané prevádzkové použitia zohrávajú kľúčovú úlohu pri identifikácii takýchto potenciálnych príčin.
86. Takisto je potrebné posúdiť závažnosť týchto rizík pre dotknuté osoby. Okrem iného možno zvážiť, ako sa osobné údaje spracúvajú (napr. ak sa kombinujú s inými súbormi údajov), aký je rozsah spracúvania a množstvo spracúvaných osobných údajov⁶⁸ (napr. celkový objem údajov, objem údajov na dotknutú osobu, počet ovplyvnených dotknutých osôb)⁶⁹, postavenie dotknutej osoby (napr. deti alebo iné zraniteľné dotknuté osoby) a ich vzťah k prevádzkovateľovi (napr. ak je dotknutá osoba zákazníkom). Napríklad používanie extrahovania údajov z webu vo fáze vývoja môže viesť - pri absencii dostatočných bezpečnostných opatrení - k významným vplyvom na jednotlivcov z dôvodu veľkého objemu získaných údajov, veľkého počtu dotknutých osôb a nerozlišujúceho zberu osobných údajov.

⁶⁶ Pozri usmernenia EDPB 1/2024 k spracúvaniu osobných údajov na základe článku 6 ods. 1 písm. f) všeobecného nariadenia o ochrane údajov, verzia 1.0, prijaté 8. októbra 2024, bod 39.

⁶⁷ Pozri usmernenia EDPB 1/2024 k spracúvaniu osobných údajov na základe článku 6 ods. 1 písm. f) všeobecného nariadenia o ochrane údajov, verzia 1.0, prijaté 8. októbra 2024, bod 32.

⁶⁸ Pozri usmernenia EDPB 1/2024 k spracúvaniu osobných údajov na základe článku 6 ods. 1 písm. f) všeobecného nariadenia o ochrane údajov, verzia 1.0, prijaté 8. októbra 2024, bod 43.

⁶⁹ Rozsudok SDEÚ zo 4. júla 2023, vec C-252/21, *Meta v. Bundeskartellamt* (ECLI:EU:C:2023:537), bod 116.

87. **Ďalšie dôsledky**, ktoré spracúvanie môže mať, by sa takisto mali zohľadniť pri posudzovaní vplyvu spracúvania na dotknuté osoby. Dozorné orgány by ich mali posudzovať od prípadu k prípadu s prihliadnutím na konkrétne skutočnosti, o ktoré ide.
88. Takéto dôsledky môžu zahŕňať (ale neobmedzujú sa len na) riziká porušenia základných práv dotknutých osôb, ako sa uvádza v predchádzajúcom pododdieli⁷⁰. Riziká sa môžu líšiť, pokiaľ ide o ich pravdepodobnosť a závažnosť, a môžu vyplývať zo spracúvania osobných údajov, ktoré by mohlo viesť k fyzickej, materiálnej alebo nemateriálnej škode, najmä ak spracúvanie môže viesť k diskriminácii⁷¹.
89. Ak nasadenie modelu umelej inteligencie zahŕňa spracúvanie osobných údajov i) dotknutých osôb, ktorých osobné údaje sú zahrnuté do súboru údajov použitého vo fáze vývoja, a ii) dotknutých osôb, ktorých osobné údaje sa spracúvajú vo fáze nasadzovania, dozorné orgány by mali pri overovaní testu vyváženosti vykonaného prevádzkovateľom rozlišovať a zvážiť riziká ovplyvňujúce záujmy, práva a slobody každej z týchto kategórií dotknutých osôb.
90. **V analýze možných ďalších dôsledkov spracúvania by sa napokon mala zvážiť aj pravdepodobnosť, že sa tieto ďalšie dôsledky prejavia.** Posúdenie takejto pravdepodobnosti by sa malo vykonať s prihliadnutím na zavedené technické a organizačné opatrenia a osobitné okolnosti prípadu. Dozorné orgány môžu napríklad zvážiť, či boli vykonané opatrenia na zabránenie potenciálnemu zneužitiu modelu umelej inteligencie. V prípade modelov umelej inteligencie, ktoré sa môžu nasadzovať na rôzne účely, ako je generatívna umelá inteligencia, to môže zahŕňať kontroly, ktorými sa v čo najväčšej miere obmedzuje ich používanie na škodlivé praktiky, napríklad: vytváranie deepfakes (vysoko falošný obsah), chatboty, ktoré sa používajú na dezinformácie, phishing a iné druhy podvodov, a manipulatívne činnosti umelej inteligencie/UI (najmä ak sú antropomorfné alebo poskytujú zavádzajúce informácie).

Primerané očakávania dotknutých osôb

91. Na základe odôvodnenia 47 GDPR, „[e]xistencia oprávneného záujmu by si v každom prípade vyžadovala dôkladné posúdenie vrátane posúdenia toho, či dotknutá osoba môže v danom čase a kontexte získavania osobných údajov primerane očakávať, že sa spracúvanie na tento účel môže uskutočniť. Záujmy a základné práva dotknutej osoby by mohli prevážiť nad záujmami prevádzkovateľa údajov najmä vtedy, ak sa osobné údaje spracúvajú za okolností, keď dotknuté osoby primerane neočakávajú ďalšie spracúvanie“⁷².
92. Primerané očakávania zohrávajú kľúčovú úlohu pri teste vyváženosti, a to v neposlednom rade z dôvodu zložitosti technológie použitej v modeloch umelej inteligencie a skutočnosti, že pre dotknuté osoby môže byť ťažké pochopiť rozmanitosť potenciálnych použití modelu umelej inteligencie a príslušného spracúvania údajov⁷³. Na tento účel sa môžu informácie poskytnuté dotknutým osobám

⁷⁰ Pozri pododdiel „Záujmy, základné práva a slobody dotknutých osôb“ vyššie.

⁷¹ Pozri oddiel 2.3 usmernení EDPB 1/2024 o spracúvaní osobných údajov na základe článku 6 ods. 1 písm. f) všeobecného nariadenia o ochrane údajov, verzia 1.0 prijatá 8. októbra 2024. Ďalšie príklady pozri aj v odôvodnení 75 všeobecného nariadenia o ochrane údajov.

⁷² Pozri tiež rozsudok SDEÚ zo 4. júla 2023, vec C-252/21, *Meta v. Bundeskartellamt* (ECLI:EU:C:2023:537), bod 112; SDEÚ, rozsudok z 11. decembra 2019, vec C-708/18, *Asociația de Proprietari bloc M5A-ScaraA* (ECLI:EU:C:2019:1064), bod 58; SDEÚ, rozsudok zo 4. októbra 2024, C-621/22, *Koninklijke Nederlandse Lawn Tennisbond* (ECLI:EU:C:2024:857), bod 55.

⁷³ Napríklad v rozsudku zo 4. júla 2023, vec C-252/21, *Meta v. Bundeskartellamt* (ECLI:EU:C:2023:537), bod 123, SDEÚ síce konštatoval, že „zlepšenie produktu“ v zásade nemožno vylúčiť ako oprávnený záujem, ale zároveň konštatoval, že možno „pochybovať o tom, či [...] cieľ spočívajúci v zlepšení produktu - vzhľadom na rozsah tohto spracúvania a jeho významný vplyv na používateľa, ako aj na okolnosť, že používateľ nemusí odôvodnene

zohľadniť pri posudzovaní toho, či dotknuté osoby môžu primerane očakávať, že ich osobné údaje budú spracúvané. Hoci vynechanie informácií môže prispieť k tomu, že dotknuté osoby neočakávajú určité spracúvanie, samotné splnenie požiadaviek na transparentnosť stanovených vo všeobecnom nariadení o ochrane údajov samo osebe nestačí na vyvodenie záveru, že dotknuté osoby môžu primerane očakávať určité spracúvanie⁷⁴. Okrem toho, jednoducho preto, že informácie týkajúce sa fázy vývoja modelu umelej inteligencie sú zahrnuté do politiky ochrany osobných údajov prevádzkovateľa, nevyhnutne to neznamena, že dotknuté osoby môžu primerane očakávať, že sa to stane; dozorné orgány by to skôr mali analyzovať vzhľadom na osobitné okolnosti prípadu a so zreteľom na všetky relevantné faktory.

93. Pri posudzovaní primeraných očakávaní dotknutých osôb v súvislosti so spracúvaním, ktoré sa uskutočňuje vo fáze vývoja, je dôležité odvolať sa na prvky uvedené v usmerneniach EDPB o oprávnenom záujme⁷⁵. Okrem toho je v rámci predmetu tohto stanoviska dôležité zvážiť širší kontext spracúvania. To môže zahŕňať, aj keď sa to na to neobmedzuje, či osobné údaje boli alebo neboli verejne dostupné, povahu vzťahu medzi dotknutou osobou a prevádzkovateľom (a či existuje medzi nimi prepojenie), povahu služby, kontext, v ktorom boli osobné údaje získané, zdroj, z ktorého boli údaje získané (napr. webové sídlo alebo služba, kde boli osobné údaje získané, a nastavenia ochrany súkromia, ktoré ponúkajú), možné ďalšie použitia modelu a či dotknuté osoby skutočne vedia, že ich osobné údaje sú vôbec online.
94. Vo fáze vývoja modelu sa primerané očakávania dotknutých osôb môžu líšiť v závislosti od toho, či údaje spracúvané na účely vývoja modelu zverejňujú dotknuté osoby alebo nie. Okrem toho sa primerané očakávania môžu líšiť aj v závislosti od toho, či údaje poskytli priamo prevádzkovateľovi (napr. v súvislosti s používaním služby), alebo či ich prevádzkovateľ získal z iného zdroja (napr. prostredníctvom tretej strany alebo extrahovania údajov). V oboch prípadoch by sa pri posudzovaní primeraných očakávaní mali zohľadniť kroky prijaté na informovanie dotknutých osôb o spracovateľských činnostiach.
95. Vo fáze nasadzovania modelu umelej inteligencie je rovnako dôležité zohľadniť primerané očakávania dotknutých osôb v kontexte osobitných spôsobilostí modelu. Napríklad v prípade modelov umelej inteligencie, ktoré sa môžu prispôbovať podľa poskytnutých vstupov, môže byť relevantné zvážiť, či si dotknuté osoby boli vedomé, že poskytli osobné údaje, aby model umelej inteligencie mohol prispôbiť svoje reakcie ich potrebám a aby mohli získať služby na mieru. Ďalej môže byť relevantné zvážiť, či by táto spracovateľská činnosť mala vplyv len na službu poskytovanú dotknutým osobám (napr. personalizácia obsahu pre konkrétného používateľa), alebo či by sa použila na úpravu služby poskytovanej všetkým zákazníkom (napr. na všeobecné zlepšenie modelu). Rovnako ako vo fáze vývoja môže byť mimoriadne dôležité zvážiť, či existuje priame prepojenie medzi dotknutými osobami a prevádzkovateľom. Takéto priame prepojenie môže napríklad umožniť prevádzkovateľovi ľahko poskytnúť dotknutým osobám informácie o spracovateľskej činnosti a modeli, ktoré by potom mohli ovplyvniť primerané očakávania týchto dotknutých osôb.

Zmierňujúce opatrenia

96. Ak sa zdá, že záujmy, práva a slobody dotknutých osôb prevažujú nad oprávnenými záujmami prevádzkovateľa alebo tretej strany, prevádzkovateľ môže zvážiť zavedenie zmierňujúcich opatrení

očakávať, že tieto údaje budú spracúvať [...] - prednosť pred záujmami a základnými právami takéhoto používateľa, a to o to viac, ak sú týmito používateľmi deti”.

⁷⁴ Usmernenia 1/2024 k spracúvaniu osobných údajov na základe článku 6 ods. 1 písm. f) všeobecného nariadenia o ochrane údajov, verzia 1.0, prijaté 8. októbra 2024, bod 53.

⁷⁵ Usmernenia 1/2024 o spracúvaní osobných údajov na základe článku 6 ods. 1 písm. f) všeobecného nariadenia o ochrane údajov, verzia 1.0, prijaté 8. októbra 2024, body 50 – 54.

na obmedzenie vplyvu spracúvania na tieto dotknuté osoby. Zmierňujúce opatrenia sú záruky, ktoré by mali byť prispôsobené okolnostiam prípadu a závisieť od rôznych faktorov vrátane zamýšľaného použitia modelu umelej inteligencie. Cieľom týchto zmierňujúcich opatrení by bolo zabezpečiť, aby záujmy prevádzkovateľa alebo tretej strany neboli prevážené, takže prevádzkovateľ by sa mohol spoliehať na tento právny základ.

97. Ako sa pripomína v usmerneniach EDPB k oprávnenému záujmu, zmierňujúce opatrenia by sa nemali zamieňať s opatreniami, ktoré je prevádzkovateľ zo zákona povinný prijať aj tak, aby sa zabezpečil súlad so všeobecným nariadením o ochrane údajov, bez ohľadu na to, či je spracúvanie založené na článku 6 ods. 1 písm. f) všeobecného nariadenia o ochrane údajov⁷⁶. Je to obzvlášť dôležité v prípade opatrení, ktoré si napríklad vyžadujú súlad so zásadami stanovenými vo všeobecnom nariadení o ochrane údajov, ako je zásada minimalizácie údajov.
98. Nižšie uvedený zoznam opatrení nie je vyčerpávajúci a normatívny a vykonávanie opatrení by sa malo posudzovať individuálne v každom prípade. Hoci v závislosti od okolností môžu byť niektoré z ďalej uvedených opatrení potrebné na splnenie osobitných povinností vyplývajúcich zo všeobecného nariadenia o ochrane údajov, ak to tak nie je, môžu sa zohľadniť ako dodatočné záruky. Okrem toho sa niektoré z ďalej uvedených opatrení týkajú oblastí, ktoré podliehajú rýchlemu a novému vývoju, a dozorné orgány by ich mali zohľadniť pri riešení konkrétného prípadu.
99. **V súvislosti s fázou vývoja modelov umelej inteligencie** možno prijať niekoľko opatrení na zmiernenie rizík, ktoré predstavuje spracúvanie údajov prvej strany, ako aj údajov tretej strany (vrátane zmiernenia rizík súvisiacich s postupmi extrahovania údajov z webu). Na základe uvedených skutočností EDPB poskytuje niekoľko príkladov opatrení, ktoré možno zaviesť na zmiernenie rizík zistených pri teste vyváženosti, a dozorné orgány by ich mali zohľadniť pri posudzovaní konkrétnych modelov umelej inteligencie na individuálnom základe.
100. **Technické opatrenia:**
- a. Opatrenia uvedené v oddiele 3.2.2, ktoré sú vhodné na zmiernenie príslušných rizík, ak tieto opatrenia nemajú za následok anonymizáciu modelu a nevyžadujú sa na splnenie iných povinností podľa všeobecného nariadenia o ochrane údajov alebo na základe testu nevyhnutnosti (druhý krok posúdenia oprávneného záujmu).
101. Okrem týchto opatrení môžu byť relevantné aj ďalšie opatrenia:
- b. opatrenia na pseudonymizáciu: mohli by zahŕňať napríklad opatrenia na zabránenie akejkoľvek kombinácii údajov na základe individuálnych identifikátorov. Tieto opatrenia nemusia byť vhodné, ak sa dozorný orgán domnieva, že prevádzkovateľ preukázal primeranú potrebu získať rôzne údaje o konkrétnej osobe na účely vývoja dotknutého systému alebo modelu umelej inteligencie.
 - c. Opatrenia na maskovanie osobných údajov alebo ich nahradenie falošnými osobnými údajmi v tréningovom súbore údajov (napr. nahradenie mien a e-mailových adries falošnými menami a falošnými e-mailovými adresami). Toto opatrenie môže byť obzvlášť vhodné, ak skutočný obsah údajov nie je relevantný pre celkové spracúvanie (napr. pri tréningu LLM).
102. **Opatrenia, ktoré uľahčujú výkon práv jednotlivcov:**

⁷⁶ Usmernenia 1/2024 k spracúvaniu osobných údajov na základe článku 6 ods. 1 písm. f) všeobecného nariadenia o ochrane údajov, verzia 1.0, prijaté 8. októbra 2024, bod 57.

- a. dodržiavanie primeraného časového obdobia medzi získavaním tréningových údajov a jeho používaním. Táto dodatočná záruka môže dotknutým osobám umožniť uplatňovať svoje práva počas tohto obdobia, pričom primeraná lehota sa posudzuje v závislosti od okolností každého prípadu.
- b. Navrhnutie bezpodmienečného „odmietnutia“ od začiatku, napríklad poskytnutím práva na voľné uváženie namietat' dotknutým osobám pred uskutočnením spracúvania, s cieľom posilniť kontrolu fyzických osôb nad ich údajmi, čo presahuje rámec podmienok článku 21 všeobecného nariadenia o ochrane údajov⁷⁷.
- c. Umožnenie dotknutým osobám uplatniť svoje právo na vymazanie, aj keď sa neuplatňujú osobitné dôvody uvedené v článku 17 ods. 1 všeobecného nariadenia o ochrane údajov⁷⁸.
- d. Umožnenie dotknutým osobám predložiť požiadavky týkajúce sa regurgitácie alebo zapamätania si osobných údajov a okolností a prostriedky, na základe ktorých možno tieto požiadavky reprodukovať, čo prevádzkovateľom umožní reprodukovať a posúdiť príslušné techniky „odučenia“ v záujme riešenia týchto požiadaviek.

103. **Opatrenia na zabezpečenie transparentnosti:** v niektorých prípadoch by zmierňujúce opatrenia mohli zahŕňať opatrenia, ktorými sa zabezpečí väčšia transparentnosť, pokiaľ ide o vývoj modelu umelej inteligencie. Niektoré opatrenia môžu okrem dodržiavania povinností vyplývajúcich zo všeobecného nariadenia o ochrane údajov pomôcť prekonať informačnú asymetriu a umožniť dotknutým osobám lepšie pochopiť spracúvanie, ktoré je súčasťou fázy vývoja:

- a. Zverejnenie verejnej a ľahko dostupnej komunikácie, ktorá presahuje rámec informácií požadovaných podľa článku 13 alebo 14 všeobecného nariadenia o ochrane údajov, napríklad poskytnutím ďalších podrobností o kritériách získavania a všetkých použitých súboroch údajov, so zohľadnením osobitnej ochrany detí a zraniteľných osôb.
- b. Alternatívne formy informovania dotknutých osôb, napríklad: mediálne kampane s rôznymi médiami na informovanie dotknutých osôb, informačná kampaň prostredníctvom e-mailu, používanie grafickej vizualizácie, často kladené otázky, označenia transparentnosti a vzorové karty, ktorých systematizácia by mohla štruktúrovať prezentáciu informácií o modeloch umelej inteligencie, a výročné správy o transparentnosti na dobrovoľnom základe.

104. **Špecifické zmierňujúce opatrenia v súvislosti s extrahovaním údajov z webu:** Vzhľadom na to, že, ako bolo uvedené vyššie, s extrahovaním údajov z webu súvisia špecifické riziká⁷⁹, by sa mohli v tejto súvislosti určiť špecifické zmierňujúce opatrenia. Ak je to relevantné, dozorné orgány ich môžu okrem uvedených zmierňujúcich opatrení zvážiť aj pri vyšetrovaní prevádzkovateľov vykonávajúcich extrahovanie údajov z webu.

105. Osobitné opatrenia, ak nie sú potrebné v rámci druhého kroku posúdenia oprávneného záujmu, sa môžu ukázať ako užitočné na zmiernenie rizika v kontexte extrahovania údajov z webu. Môžu zahŕňať **technické opatrenia**, ako napríklad:

⁷⁷ Tamže.

⁷⁸ Tamže.

⁷⁹ Tieto praktiky môžu vyvolávať aj ďalšie otázky, ktoré nie sú predmetom tohto stanoviska, pozri napríklad Pagallo U., Ciani Sciolla J., *Anatómia extrahovania údajov z webu: etika, normy a problémy práva*. European Journal of Privacy Law & Technologies, (2023) 2 s. 1 - 19, dostupné na: <https://doi.org/10.57230/EJPLT232PS>.

- a. Vylúčenie dátového obsahu z publikácií, ktorý by mohol zahŕňať osobné údaje predstavujúce riziká pre konkrétne osoby alebo skupiny osôb (napr. jednotlivci, ktorí by mohli byť vystavení zneužívaniu, predsudkom alebo dokonca fyzickej ujme, ak by sa informácie zverejnili).
 - b. Zabezpečenie toho, aby sa určité kategórie údajov nezískavali alebo aby sa určité zdroje vylúčili zo získavania údajov; to by mohlo zahŕňať napríklad určité webové stránky, ktoré sú obzvlášť rušivé vzhľadom na citlivosť ich predmetu.
 - c. Vylúčenie získavania z webových stránok (alebo častí webových stránok), ktoré jasne namietajú proti extrahovaniu údajov z webu a opätovnému použitiu ich obsahu na účely vytvárania databáz na tréovanie umelej inteligencie (napríklad rešpektovaním súborov robots.txt alebo ai.txt alebo akéhokoľvek iného uznávaného mechanizmu na vyjadrenie vylúčenia z automatizovaného prehľadávania alebo extrahovania údajov).
 - d. Zavedenie ďalších relevantných obmedzení získavania, prípadne vrátane kritérií založených na časových obdobiach.
106. V kontexte extrahovania údajov z webu môžu príklady konkrétnych opatrení **uľahčujúcich výkon práv fyzických osôb a transparentnosť** zahŕňať: vytvorenie zoznamu subjektov, ktoré si neželajú spracúvanie ich údajov, ktorý spravuje prevádzkovateľ a ktorý umožňuje dotknutým osobám namietat proti zhromažďovaniu ich údajov na určitých webových stránkach alebo online platformách poskytnutím informácií, ktoré ich identifikujú na týchto webových stránkach, a to aj pred získavaním údajov⁸⁰.
107. **Osobitné úvahy týkajúce sa zmierňujúcich opatrení vo fáze nasadzovania:** Hoci niektoré z uvedených opatrení môžu byť relevantné aj pre fázu nasadzovania, EDPB v závislosti od okolností ďalej uvádza neúplný zoznam ďalších podporných opatrení, ktoré sa môžu zaviesť a ktoré by mali posúdiť dozorné orgány v každom jednotlivom prípade.
- a. Môžu sa zaviesť napríklad **technické opatrenia** na predchádzanie uchovávaniu, regurgitácii alebo generovaniu osobných údajov, najmä v kontexte modelov generatívnej umelej inteligencie (ako sú výstupné filtre), a/alebo na zmiernenie rizika nezákonného opätovného použitia modelmi umelej inteligencie na všeobecné účely (napr. digitálne vodoznakovanie výstupov vytvorených umelou inteligenciou).
 - b. **Opatrenia, ktoré uľahčujú alebo urýchľujú výkon práv fyzických osôb** vo fáze nasadzovania nad rámec toho, čo sa vyžaduje podľa zákona, týkajúce sa najmä, a nielen, výkonu práva na vymazanie osobných údajov z výstupných údajov modelu alebo deduplikácie a techník po dokončení tréovania, ktoré sa snažia odstrániť alebo potlačiť osobné údaje.
108. Pri vyšetrovaní nasadzovania konkrétného modelu umelej inteligencie by dozorné orgány mali zvážiť, či prevádzkovateľ uverejnil test vyváženosti, ktorý vykonal, keďže sa tým môže zvýšiť transparentnosť a spravodlivosť. Ako sa uvádza v usmerneniach EDPB o oprávnených záujmoch, môžu sa zvážiť iné opatrenia s cieľom poskytnúť dotknutým osobám informácie z testu vyváženosti pred akýmkoľvek

⁸⁰ Pokiaľ prevádzkovateľ nepreukáže nevyhnutné oprávnené dôvody na spracúvanie, ktoré prevažujú nad záujmami, právami a slobodami dotknutej osoby, alebo dôvody na preukazovanie, uplatňovanie alebo obhajovanie právnych nárokov.

získavaním osobných údajov⁸¹. EDPB tiež pripomína⁸², že prvkom, ktorý sa má zvážiť, je, či prevádzkovateľ v prípade potreby zapojil zodpovednú osobu.

3.4 O možnom vplyve nezákonného spracúvania pri vývoji modelu umelej inteligencie na zákonnosť následného spracúvania alebo prevádzky modelu umelej inteligencie

109. Táto časť stanoviska sa zaoberá otázkou č. 4 žiadosti. Cieľom tejto otázky je objasniť možný vplyv nezákonného spracúvania vo fáze vývoja na následné spracúvanie (napríklad vo fáze nasadzovania modelu umelej inteligencie) alebo na prevádzku modelu. Cieľom otázky je riešiť situáciu, keď takýto model umelej inteligencie spracúva osobné údaje, ktoré sa uchovávajú v modeli (otázka 4 písm. i) žiadosti), ako aj situáciu, keď sa už do nasadenia modelu umelej inteligencie nezapája žiadne spracúvanie osobných údajov (t. j. model je anonymný) (otázka č. 4 bod ii) žiadosti).
110. Predtým, ako sa začne zaoberať niektorými konkrétnymi scenármi, EDPB uvádza tieto všeobecné úvahy.
111. Po prvé, objasnenia uvedené v tejto časti sa budú zameriavať na spracúvanie osobných údajov vo fáze vývoja vykonávané pri nedodržaní zásady zákonnosti stanovenej konkrétne v článku 5 ods. 1 písm. a) a článku 6 všeobecného nariadenia o ochrane údajov (ďalej len „nezákonnosť“)⁸³. V rovnakom duchu sa úvahy EDPB zamerajú na vplyv nezákonnosti spracúvania vo fáze vývoja na zákonnosť (t. j. súlad s článkom 5 ods. 1 písm. a) všeobecného nariadenia o ochrane údajov a článkom 6 všeobecného nariadenia o ochrane údajov) následného spracúvania alebo prevádzky modelu. EDPB však poukazuje na to, že spracúvanie vykonávané vo fáze vývoja môže viesť aj k porušeniam iných ustanovení všeobecného nariadenia o ochrane údajov, ako je nedostatočná transparentnosť voči dotknutým osobám alebo špecificky navrhnutá a/alebo štandardná ochrana údajov, ktoré nie sú analyzované v tomto stanovisku.
112. Po druhé, pri riešení tejto otázky zohráva kľúčovú úlohu zásada zodpovednosti, ktorá vyžaduje, aby prevádzkovatelia boli zodpovední, *okrem iného*, za článok 5 ods. 1 všeobecného nariadenia o ochrane údajov a článok 6 všeobecného nariadenia o ochrane údajov⁸⁴ a preukázali s nimi súlad. Platí to aj pre potrebu posúdiť, ktorá organizácia je prevádzkovateľom predmetnej spracovateľskej činnosti, a či dochádza k situáciám spoločných prevádzkovateľov (keďže môžu byť neoddeliteľne prepojení)⁸⁵. Vzhľadom na význam skutkových okolností každého prípadu, a to aj pokiaľ ide o úlohu, ktorú zohráva každá strana zapojená do spracúvania, by sa úvahy EDPB mali chápať ako všeobecné pripomienky, ktoré by dozorné orgány mali posudzovať od prípadu k prípadu.
113. Po tretie, EDPB zdôrazňuje, že v súlade s článkom 51 ods. 1 všeobecného nariadenia o ochrane údajov sú dozorné orgány „zodpovedné za monitorovanie uplatňovania [všeobecného nariadenia o ochrane údajov] s cieľom chrániť základné práva a slobody fyzických osôb pri spracúvaní a uľahčiť voľný tok osobných údajov v rámci Únie“. Je preto v právomoci dozorných orgánov posudzovať zákonnosť

⁸¹ Usmernenia EDPB 1/2024 k spracúvaniu osobných údajov na základe článku 6 ods. 1 písm. f) všeobecného nariadenia o ochrane údajov, verzia 1.0, prijaté 8. októbra 2024, bod 68.

⁸² Usmernenia EDPB 1/2024 k spracúvaniu osobných údajov na základe článku 6 ods. 1 písm. f) všeobecného nariadenia o ochrane údajov, verzia 1.0, prijaté 8. októbra 2024, bod 12.

⁸³ SDEÚ, rozsudok zo 4. mája 2023, vec C-60/22, *Bundesrepublik Deutschland* (ECLI:EU:C:2023:373), body 55 – 57.

⁸⁴ SDEÚ, rozsudok zo 4. mája 2023, vec C-60/22, *Bundesrepublik Deutschland* (ECLI:EU:C:2023:373), bod 53.

⁸⁵ Usmernenia EDPB 07/2020 k pojmom prevádzkovateľ a sprostredkovateľ podľa všeobecného nariadenia o ochrane údajov, verzia 2.1, prijaté 7. júla 2021, bod 55.

spracúvania a vykonávať svoje právomoci udelené vo všeobecnom nariadení o ochrane údajov v súlade s ich vnútroštátnym rámcom⁸⁶. V takýchto prípadoch majú dozorné orgány diskrečnú právomoc posúdiť možné porušenie (porušenia) a vybrať vhodné, potrebné a primerané opatrenia spomedzi opatrení uvedených v článku 58 všeobecného nariadenia o ochrane údajov, pričom zohľadnia okolnosti každého jednotlivého prípadu⁸⁷.

114. **Ak sa zistí porušenie, dozorné orgány môžu zaviesť nápravné opatrenia, ako napríklad nariadiť prevádzkovateľom, aby s prihliadnutím na okolnosti každého prípadu prijali opatrenia na nápravu nezákonnosti počítačného spracúvania.** Môžu zahŕňať napríklad udelenie pokuty, uloženie dočasného obmedzenia spracúvania, vymazanie časti súboru údajov, ktorý bol spracúvaný nezákonne, alebo, ak to nie je možné, v závislosti od konkrétnych skutočností, so zreteľom na primeranosť opatrenia, nariadenie vymazania celého súboru údajov použitého na vývoj modelu umelej inteligencie a/alebo samotného modelu umelej inteligencie. Pri posudzovaní primeranosti plánovaného opatrenia môžu dozorné orgány zohľadniť opatrenia, ktoré môže prevádzkovateľ uplatniť na nápravu nezákonnosti počítačného spracúvania (napr. opätovné tréningovanie).
115. EDPB takisto zdôrazňuje, že ak sa osobné údaje spracúvajú nezákonne, dotknuté osoby môžu požiadať o vymazanie svojich osobných údajov za podmienok stanovených v článku 17 všeobecného nariadenia o ochrane údajov a že dozorné orgány môžu nariadiť vymazanie osobných údajov *ex officio*⁸⁸.
116. Pri posudzovaní toho, či je opatrenie vhodné, nevyhnutné a primerané, môžu dozorné orgány okrem iného zvážiť riziká pre dotknuté osoby, závažnosť porušenia, technickú a finančnú uskutočniteľnosť opatrenia, ako aj objem dotknutých osobných údajov.
117. EDPB napokon pripomína, že opatreniami prijatými dozornými orgánmi podľa všeobecného nariadenia o ochrane údajov nie sú dotknuté opatrenia prijaté príslušnými orgánmi podľa aktu o umelej inteligencii a/alebo podľa iných uplatniteľných právnych rámcov (napr. právnych predpisov o občianskoprávnej zodpovednosti).
118. V nasledujúcich častiach sa EDPB bude zaoberať tromi scenármi, na ktoré sa vzťahuje otázka č. 4 žiadosti, pričom rozdiely spočívajú v tom, či sa osobné údaje spracúvané na účely vývoja modelu uchovávali v modeli a/alebo či následné spracúvanie vykonáva ten istý alebo iný prevádzkovateľ.

3.4.1 Scenár 1 Prevádzkovateľ neoprávnene spracúva osobné údaje na účely vývoja modelu, osobné údaje sa uchovávali v modeli a následne ich spracúva ten istý prevádzkovateľ (napríklad v súvislosti s nasadením modelu)

119. Tento scenár sa týka otázky č. 4 písm. i) žiadosti v situácii, keď prevádzkovateľ nezákonne spracúva osobné údaje (t. j. nedodržaním článku 5 ods. 1 písm. a) všeobecného nariadenia o ochrane údajov a

⁸⁶ Môže byť potrebné zohľadniť osobitné vnútroštátne pravidlá. Pozri napríklad článok 2-decies talianskeho zákonníka o ochrane údajov (legislatívny dekrét 196/2003), v ktorom sa stanovuje, že údaje spracúvané v rozpore s pravidlami ochrany údajov nemožno použiť. Týmto nie sú dotknuté iné vnútroštátne právne rámce, napríklad trestné zákony.

⁸⁷ V tejto súvislosti pozri odôvodnenie 129 všeobecného nariadenia o ochrane údajov, ako aj rozsudok SDEÚ z 26. septembra 2024, vec C-768-21, *TR/Land Hessen* (ECLI:EU:C:2024:785), bod 37; rozsudok SDEÚ zo 7. decembra 2023, v spojených veciach C-26/22 a C-64/22, *SCHUFA Holding (Libération de reliquat de dette)* (ECLI:EU:C:2023:958), bod 57; a rozsudok SDEÚ zo 14. marca 2024, vec C-46/23, *Újpesti Polgármesteri Hivatal* (ECLI:EU:C:2024).

⁸⁸ V tejto súvislosti stanovisko EDPB 39/2021 k tomu, či by článok 58 ods. 2 písm. g) všeobecného nariadenia o ochrane údajov mohol slúžiť ako právny základ na to, aby dozorný orgán nariadil *ex officio* vymazanie osobných údajov v situácii, keď takúto žiadosť dotknutá osoba nepredložila, bod 28. V tejto súvislosti pozri aj rozsudok Súdneho dvora zo 14. marca 2024, vec C-46/23, *Újpesti Polgármesteri Hivatal* (ECLI:EU:C:2024:239), bod 42.

článku 6 všeobecného nariadenia o ochrane údajov) na účely vývoja modelu umelej inteligencie, model umelej inteligencie uchováva informácie týkajúce sa identifikovanej alebo identifikovateľnej fyzickej osoby, a preto nie je anonymný. Osobné údaje potom následne spracúva ten istý prevádzkovateľ (napríklad v súvislosti s nasadením modelu). V súvislosti s týmto scenárom EDPB uvádza nasledovné úvahy.

120. Právomoc dozorného orgánu uložiť nápravné opatrenia týkajúce sa pôvodného spracúvania (ako je vysvetlené v bodoch 113, 114 a 115 vyššie) by v zásade mala vplyv na následné spracúvanie (napr. ak dozorný orgán nariadi prevádzkovateľovi vymazať osobné údaje, ktoré boli spracúvané nezákonne, takéto nápravné opatrenia by prevádzkovateľovi neumožnili následne spracúvať osobné údaje, ktoré boli predmetom opatrení).
 121. Pokiaľ ide konkrétne o vplyv nezákonného spracúvania vo fáze vývoja na následné spracúvanie (napríklad vo fáze nasadenia), EDPB pripomína, že je úlohou dozorných orgánov vykonať analýzu jednotlivých prípadov, ktorá zohľadňuje špecifické okolnosti každého prípadu.
 122. **To, či fázy vývoja a nasadzovania zahŕňajú samostatné účely (teda predstavujú samostatné spracovateľské činnosti) a rozsah, v akom nedostatok právneho základu pre počiatočnú spracovateľskú činnosť ovplyvňuje zákonnosť následného spracúvania, by sa mali posudzovať od prípadu k prípadu v závislosti od kontextu prípadu.**
 123. Napríklad s osobitným zreteľom na právny základ článku 6 ods. 1 písm. f) všeobecného nariadenia o ochrane údajov, ak je následné spracúvanie založené na oprávnenom záujme, pri posúdení oprávneného záujmu by sa mala zohľadniť skutočnosť, že počiatočné spracúvanie bolo nezákonné (napr. pokiaľ ide o riziká pre dotknuté osoby alebo skutočnosť, že dotknuté osoby nemusia očakávať takéto následné spracúvanie). V týchto prípadoch môže mať nezákonnosť spracúvania vo fáze vývoja vplyv na zákonnosť následného spracúvania.
- 3.4.2 Scenár 2 Prevádzkovateľ neoprávnene spracúva osobné údaje na účely vývoja modelu, osobné údaje sa uchovávajú v modeli a spracúva ich iný prevádzkovateľ v súvislosti s nasadením modelu
124. Tento scenár sa týka otázky č. 4 písm. i) žiadosti. Líši sa od scenára 1 (v oddiele 3.4.1 tohto stanoviska), keďže osobné údaje následne spracúva iný prevádzkovateľ v kontexte nasadzovania modelu umelej inteligencie.
 125. EDPB pripomína, že zistenie úloh pridelených týmto rôznym aktérom v rámci ochrany údajov je nevyhnutným krokom na určenie toho, ktoré povinnosti podľa všeobecného nariadenia o ochrane údajov sa uplatňujú a kto je za tieto povinnosti zodpovedný, a že pri posudzovaní povinností každej strany podľa všeobecného nariadenia o ochrane údajov by sa mali zohľadniť aj situácie spoločného prevádzkovateľa. Pripomienky uvedené ďalej by sa preto mali považovať za všeobecné prvky, ktoré by dozorné orgány mali zohľadniť tam, kde je to relevantné. Pokiaľ ide o tento scenár 2, EDPB uvádza nasledovné úvahy.
 126. Po prvé, treba pripomenúť, že podľa článku 5 ods. 1 písm. a) všeobecného nariadenia o ochrane údajov v spojení s článkom 5 ods. 2 všeobecného nariadenia o ochrane údajov by mal každý prevádzkovateľ zabezpečiť zákonnosť spracúvania, ktoré vykonáva, a byť schopný ju preukázať. Dozorné orgány by preto mali posúdiť zákonnosť spracúvania vykonávaného i) prevádzkovateľom, ktorý pôvodne vyvinul model umelej inteligencie, a ii) prevádzkovateľom, ktorý nadobudol model umelej inteligencie a sám spracúva osobné údaje.

127. Po druhé, úvahy vykonané podľa odsekov 113, 114 a 115 sú v tomto prípade relevantné, pokiaľ ide o právomoc dozorných orgánov zasiahnuť v súvislosti s počiatočným spracúvaním. Článok 17 ods. 1 písm. d) všeobecného nariadenia o ochrane údajov (vymazanie nezákonne spracúvaných údajov) a článok 19 všeobecného nariadenia o ochrane údajov (oznamovacia povinnosť týkajúca sa opravy alebo vymazania osobných údajov alebo obmedzenia spracúvania) môžu byť v závislosti od okolností prípadu takisto relevantné v tejto súvislosti, napríklad v súvislosti s oznámením, ktoré by prevádzkovateľ, ktorý vyvíja model, mal vykonať voči prevádzkovateľovi, ktorý model nasadzuje.
128. Po tretie, pokiaľ ide o možný vplyv nezákonnosti počiatočného spracúvania na následné spracúvanie, ktoré vykonáva iný prevádzkovateľ, dozorné orgány by takéto posúdenie mali vykonávať na individuálnom základe.
129. **Dozorné orgány by mali zohľadniť, či prevádzkovateľ, ktorý nasadzuje model, vykonal v rámci svojich povinností v oblasti zodpovednosti primerané posúdenie⁸⁹ na preukázanie súladu s článkom 5 ods. 1 písm. a) a článkom 6 všeobecného nariadenia o ochrane údajov s cieľom uistiť sa, že model umelej inteligencie nebol vyvinutý nezákonným spracúvaním osobných údajov.** Pri takomto hodnotení dozornými orgánmi by sa malo zohľadniť, či prevádzkovateľ posúdil niektoré nevyčerpávajúce kritériá, ako je zdroj údajov a či je model umelej inteligencie výsledkom porušenia všeobecného nariadenia o ochrane údajov, najmä ak tak stanovil dozorný orgán alebo súd, aby prevádzkovateľ používajúci model nemohol ignorovať, že pôvodné spracúvanie bolo nezákonné.
130. Prevádzkovateľ by mal zvážiť napríklad to, či údaje pochádzajú z porušenia ochrany osobných údajov, alebo či bolo spracúvanie predmetom zistenia porušenia zo strany dozorného orgánu alebo súdu. **Stupeň posúdenia prevádzkovateľa a úroveň podrobnosti očakávaná dozornými orgánmi sa môžu líšiť v závislosti od rôznych faktorov vrátane druhu a stupňa rizík vyplývajúcich zo spracúvania v modeli umelej inteligencie počas jeho nasadzovania vo vzťahu k dotknutým osobám, ktorých údaje sa použili na vývoj modelu.**
131. EDPB konštatuje, že v akte o umelej inteligencii sa od poskytovateľov vysokorizikových systémov umelej inteligencie vyžaduje, aby vypracovali EÚ vyhlásenie o zhode⁹⁰ a že takéto vyhlásenie obsahuje vyhlásenie, že príslušný systém umelej inteligencie je v súlade s právnymi predpismi EÚ o ochrane údajov⁹¹. EDPB poznamenáva, že takéto vlastné vyhlásenie nemusí predstavovať konečné zistenie súladu podľa všeobecného nariadenia o ochrane údajov. Dozorné orgány ho však môžu zohľadniť pri vyšetrovaní konkrétneho modelu umelej inteligencie.
132. Rovnaké úvahy uvedené v bode 123 vyššie sú takisto relevantné v tomto prípade. Keď dozorné orgány overujú, či a ako prevádzkovateľ posúdil vhodnosť oprávneného záujmu ako právneho základu pre spracúvanie, ktoré vykonáva, nezákonnosť počiatočného spracúvania by sa mala zohľadniť v rámci posúdenia oprávneného záujmu, napríklad posúdením potenciálnych rizík, ktoré môžu vzniknúť pre dotknuté osoby, ktorých osobné údaje boli nezákonne spracúvané pri vývoji modelu. V rámci testu vyváženosti sa musia náležite zohľadniť rôzne aspekty, či už technickej povahy (napr. existencia filtrov alebo obmedzení prístupu zavedených počas vývoja modelu, ktoré následný prevádzkovateľ nemôže obísť alebo ovplyvniť a ktoré by mohli zabrániť prístupu k osobným údajom alebo ich zverejneniu), alebo právnej povahy (napr. povaha a závažnosť nezákonnosti počiatočného spracúvania).

⁸⁹ Článok 5 ods. 2 všeobecného nariadenia o ochrane údajov a článok 24 všeobecného nariadenia o ochrane údajov.

⁹⁰ Článok 16 písm. g) a článok 47 aktu o umelej inteligencii.

⁹¹ Príloha V bod 5 k aktu o umelej inteligencii.

3.4.3 Scenár 3 Prevádzkovateľ nezákonne spracúva osobné údaje na účely vývoja modelu, potom zabezpečí anonymizáciu modelu predtým, ako ten istý alebo iný prevádzkovateľ začne ďalšie spracúvanie osobných údajov v súvislosti s nasadením modelu

133. Tento scenár súvisí s otázkou č. 4 bodom ii) žiadosti a týka sa prípadu, keď prevádzkovateľ nezákonne spracúva osobné údaje na účely vývoja modelu umelej inteligencie, ale robí to spôsobom, ktorý zabezpečuje anonymizáciu osobných údajov, predtým, ako ten istý alebo iný prevádzkovateľ začne ďalšie spracúvanie osobných údajov v súvislosti s nasadením modelu. Po prvé, EDPB pripomína, že dozorné orgány sú príslušné a majú právomoc zasiahnuť, pokiaľ ide o spracúvanie súvisiace s anonymizáciou modelu, ako aj spracúvanie vykonávané počas fázy vývoja. Dozorné orgány tak môžu v závislosti od konkrétnych okolností prípadu uložiť nápravné opatrenia na toto počiatočné spracúvanie (ako je vysvetlené v bodoch 113, 114, 115 vyššie).
134. Ak je možné preukázať, že následné fungovanie modelu umelej inteligencie nezahŕňa spracúvanie osobných údajov, EDPB sa domnieva, že všeobecné nariadenie o ochrane údajov by sa neuplatňovalo⁹². Nezákonnosť pôvodného spracúvania by preto nemala mať vplyv na následnú prevádzku modelu. EDPB však zdôrazňuje, že samotné tvrdenie o anonymite modelu nestačí na jeho vyňatie z uplatňovania všeobecného nariadenia o ochrane údajov, a konštatuje, že dozorné orgány by ho mali posúdiť, pričom by mali v jednotlivých prípadoch zohľadniť úvahy, ktoré EDPB poskytol v súvislosti s otázkou č. 1 žiadosti.
135. **Keď prevádzkovatelia následne spracúvajú osobné údaje získané počas fázy nasadzovania, po anonymizácii modelu by sa v súvislosti s týmito spracovateľskými činnosťami uplatňovalo všeobecné nariadenie o ochrane údajov. V týchto prípadoch, pokiaľ ide o všeobecné nariadenie o ochrane údajov, zákonnosť spracúvania vykonávaného vo fáze nasadzovania by nemala byť ovplyvnená nezákonnosťou počiatočného spracúvania.**

4 Záverečné pripomienky

136. Toto stanovisko je určené všetkým dozorným orgánom a bude zverejnené v súlade s článkom 64 ods. 5 písm. b) všeobecného nariadenia o ochrane údajov.

Za Európsky výbor pre ochranu údajov

predsedníčka

Anu Talus

⁹² Odôvodnenie 26 všeobecného nariadenia o ochrane údajov.