

Stanovisko sboru (podle článku 64)



**Stanovisko 28/2024 k určitým aspektům ochrany údajů
v souvislosti se zpracováním osobních údajů v kontextu
modelů umělé inteligence**

Přijato dne 17. prosince 2024

Shrnutí

Technologie umělé inteligence vytvářejí mnoho příležitostí a přinášejí mnoho výhod v celé řadě odvětví a společenských aktivit.

Ochranou základního práva na ochranu osobních údajů obecné nařízení o ochraně osobních údajů tyto příležitosti podporuje a prosazuje i jiná základní práva EU, včetně práva na svobodu myšlení, projevu a informací, práva na vzdělání nebo svobody podnikání. Obecné nařízení o ochraně osobních údajů je tak právním rámcem, který podporuje odpovědné inovace.

V této souvislosti a s ohledem na otázky ochrany osobních údajů, které tyto technologie vyvolávají, požádal irský dozorový úřad EDPB o vydání stanoviska k záležitostem s obecnou působností podle čl. 64 odst. 2 obecného nařízení o ochraně osobních údajů. Žádost se týká zpracování osobních údajů v souvislosti s fázemi vývoje a zavádění modelů umělé inteligence (dále jen „AI“). V žádosti byly konkrétně položeny tyto otázky: 1) kdy a jak lze model AI považovat za „anonymní“; 2) jak mohou správci doložit vhodnost oprávněného zájmu jako právního základu ve fázi vývoje a 3) ve fázi zavádění a 4) jaký dopad má protiprávní zpracování osobních údajů ve fázi vývoje modelu AI na následné zpracování nebo provoz modelu AI.

Pokud jde o první otázku, ve stanovisku se zmiňuje, že tvrzení o anonymitě modelu AI by měly příslušné dozorové úřady posuzovat případ od případu, neboť se EDPB domnívá, že modely AI vytrénované na základě osobních údajů nelze ve všech případech považovat za anonymní. Aby mohl být model AI považován za anonymní, měla by být jak 1) pravděpodobnost přímé (včetně pravděpodobnostní) extrakce osobních údajů týkajících se osob, jejichž osobní údaje byly použity k vývoji modelu, tak 2) pravděpodobnost extrakce, ať už úmyslné, či neúmyslné, takových osobních údajů na základě dotazů zanedbatelná, vezmeme-li v úvahu „*všechny prostředky, o nichž lze rozumně předpokládat, že je správce nebo jiná osoba použije*“.

Při provádění posouzení by dozorové úřady měly přezkoumat dokumentaci poskytnutou správcem k doložení anonymity modelu. V tomto ohledu je ve stanovisku uveden nepreskriptivní a demonstrativní výčet metod, které mohou správci použít při dokládání anonymity, a dozorové úřady je tedy mohou zohlednit při posuzování tvrzení správce o anonymitě. To se týká například přístupů, jež správci zaujali během fáze vývoje k prevenci nebo omezení shromažďování osobních údajů používaných k trénování modelů AI, jež měly přispět ke snížení identifikovatelnosti těchto údajů, k zabránění jejich extrakce nebo k poskytnutí záruky ohledně odolnosti vůči útokům na základě nejmodernější techniky.

Pokud jde o druhou a třetí otázku, stanovisko obsahuje obecné úvahy, které by dozorové úřady měly zohlednit při posuzování toho, zda se správci mohou spoléhat na oprávněný zájem jako na vhodný právní základ pro zpracování prováděné v souvislosti s vývojem a zaváděním modelů AI.

Ve stanovisku se připomíná, že neexistuje žádná hierarchie mezi právními základy stanovenými v obecném nařízení o ochraně osobních údajů a že je na správcích, aby určili vhodný právní základ pro své činnosti zpracování. Ve stanovisku se dále připomíná třístupňový test, který je třeba provést při posuzování použití oprávněného zájmu jako právního základu, tj. 1) identifikace oprávněného zájmu, který sleduje správce nebo třetí strana; 2) analýza nezbytnosti zpracování pro účely sledovaného oprávněného zájmu (sledovaných oprávněných zájmů) (označováno také jako „test nezbytnosti“); a 3) posouzení, zda nad oprávněným zájmem (oprávněnými zájmy) nepřevažují zájmy nebo základní práva a svobody subjektů údajů (označováno také jako „test vyváženosti“).

Pokud jde o první krok, ve stanovisku se připomíná, že zájem lze považovat za oprávněný, jsou-li splněna tato tři kumulativní kritéria: zájem 1) je zákonný; 2) je jasně a přesně formulován a 3) je skutečný a aktuální (tj. není spekulativní). Takový zájem může zahrnovat například vývoj modelu AI – vývoj služby konverzačního agenta na pomoc uživatelům nebo jeho zavádění – zlepšení odhalování hrozeb v informačním systému.

Pokud jde o druhý krok, ve stanovisku se připomíná, že posouzení nezbytnosti zahrnuje zvažování: 1) zda činnost zpracování umožní sledování oprávněného zájmu a 2) zda existuje méně rušivý způsob sledování tohoto zájmu. Při posuzování toho, zda je splněna podmínka nezbytnosti, by dozorové úřady měly věnovat zvláštní pozornost množství zpracovávaných osobních údajů a tomu, zda je přiměřené k prosazování daného oprávněného zájmu, a to i s ohledem na zásadu minimalizace údajů.

Pokud jde o třetí krok, ve stanovisku se připomíná, že test vyváženosti by měl být proveden s ohledem na konkrétní okolnosti jednotlivých případů. Poté je uveden přehled prvků, které mohou dozorové úřady vzít v úvahu při hodnocení, zda zájmy správce nebo třetí strany převažují nad zájmy, základními právy a svobodami subjektů údajů.

V rámci třetího kroku se ve stanovisku upozorňuje na konkrétní rizika pro základní práva, která se mohou objevit buď ve fázi vývoje, nebo ve fázi zavádění modelů AI. Rovněž se objasňuje, že zpracování osobních údajů, k němuž dochází ve fázích vývoje a zavádění modelů AI, může mít na subjekty údajů různý dopad, který může být pozitivní nebo negativní. Při posuzování tohoto dopadu mohou dozorové úřady vzít v úvahu povahu údajů zpracovávaných modely, kontext zpracování a možné další důsledky zpracování.

Ve stanovisku se dále zdůrazňuje úloha přiměřených očekávání subjektů údajů v testu vyváženosti. To může být důležité vzhledem ke složitosti technologií používaných v modelech AI a skutečnosti, že pro subjekty údajů může být obtížné pochopit rozmanitost jejich potenciálních použití, jakož i různé související činnosti zpracování. V tomto ohledu mohou informace poskytované subjektům údajů i kontext zpracování patřit k prvkům, které je třeba vzít v úvahu při posuzování toho, zda mohou subjekty údajů důvodně očekávat, že jejich osobní údaje budou zpracovány. Pokud jde o kontext, může zahrnovat tyto aspekty: zda byly osobní údaje veřejně dostupné, či nikoli, povaha vztahu mezi subjektem údajů a správcem (a zda mezi nimi existuje vazba), povaha služby, kontext, v němž byly osobní údaje shromážděny, zdroj, z něhož byly údaje shromážděny (tj. internetové stránky nebo služba, kde byly osobní údaje shromážděny, a nastavení ochrany osobních údajů, které nabízejí), potenciální další využití modelu a to, zda si subjekty údajů jsou skutečně vědomy toho, že jejich osobní údaje jsou na internetu.

Ve stanovisku se rovněž připomíná, že pokud se zdá, že zájmy, práva a svobody subjektů údajů převažují nad oprávněným zájmem (oprávněnými zájmy) správce nebo třetí strany, může správce zvážit zavedení zmírňujících opatření, aby omezil dopad zpracování na tyto subjekty údajů. Zmírňující opatření by neměla být zaměňována s opatřeními, která je správce podle právních předpisů povinen v každém případě přijmout k zajištění souladu s obecným nařízením o ochraně osobních údajů. Kromě toho by tato opatření měla být přizpůsobena okolnostem daného případu a vlastnostem modelu AI, včetně jeho zamýšleného použití. V tomto ohledu je ve stanovisku uveden demonstrativní výčet příkladů zmírňujících opatření ve vztahu k fázi vývoje (rovněž pokud jde o extrakci dat z webu, tzv. web scraping) a fázi zavádění. Zmírňující opatření mohou podléhat rychlému vývoji a měla by být přizpůsobena okolnostem daného případu. Proto zůstává na dozorových úřadech, aby v jednotlivých případech posoudily vhodnost provedených zmírňujících opatření.

Pokud jde o čtvrtou otázku, ve stanovisku se obecně připomíná, že je na správním uvážení dozorového úřadu posoudit možné (možná) porušení a zvolit vhodná, nezbytná a přiměřená opatření s přihlédnutím k okolnostem každého jednotlivého případu. Stanovisko se poté zabývá třemi scénáři.

Ve scénáři č. 1 jsou osobní údaje uchovávány v modelu AI (model tedy nelze považovat za anonymní, jak je podrobně vysvětleno v první otázce) a následně jsou zpracovány stejným správcem (například v souvislosti se zaváděním modelu). Ve stanovisku se uvádí, že otázky, zda fáze vývoje a fáze zavádění zahrnují samostatné účely (a představují tak samostatné činnosti zpracování) a do jaké míry ovlivňuje neexistence právního základu pro počáteční činnost zpracování zákonnost následného zpracování, by měly být posuzovány případ od případu v závislosti na kontextu daného případu.

Ve scénáři č. 2 jsou osobní údaje uchovávány v modelu a zpracovány jiným správcem v souvislosti se zaváděním modelu. V tomto ohledu se ve stanovisku uvádí, že by dozorové úřady měly zohlednit, zda správce, který model zavádí, provedl náležité posouzení v rámci svých povinností týkajících se odpovědnosti za doložení souladu s čl. 5 odst. 1 písm. a) a článkem 6 obecného nařízení o ochraně osobních údajů, aby se ujistil, že model AI nebyl vyvinut s využitím protiprávního zpracování osobních údajů. Toto posouzení by mělo zohlednit například zdroj osobních údajů a skutečnost, zda zpracování ve fázi vývoje bylo předmětem zjištění porušení předpisů, zejména pokud jej zjistil dozorový úřad nebo soud, a mělo by být méně či více podrobné v závislosti na rizicích, která vyvolává zpracování ve fázi zavádění.

Ve scénáři č. 3 správce protiprávně zpracovává osobní údaje za účelem vývoje modelu AI a poté zajistí jejich anonymizaci, než stejný nebo jiný správce zahájí další zpracování osobních údajů v kontextu zavádění. V tomto ohledu se ve stanovisku uvádí, že pokud lze doložit, že následný provoz modelu AI nezahrnuje zpracování osobních údajů, EDPB se domnívá, že obecné nařízení o ochraně osobních údajů by se na něj nevztahovalo. Proto by protiprávnost počátečního zpracování neměla mít vliv na následný provoz modelu. EDPB se dále domnívá, že pokud správci následně zpracovávají osobní údaje shromážděné během fáze zavádění poté, co byl model anonymizován, vztahuje se na tyto operace zpracování obecné nařízení o ochraně osobních údajů. V těchto případech se ve stanovisku vychází z toho, že pokud jde o obecné nařízení o ochraně osobních údajů, zákonnost zpracování prováděného ve fázi zavádění by neměla být dotčena protiprávností počátečního zpracování.

Obsah

1	Úvod	6
1.1	Shrnutí skutečností	6
1.2	Přípustnost žádosti o stanovisko podle čl. 64 odst. 2 obecného nařízení o ochraně osobních údajů	8
2	Oblast působnosti a klíčové pojmy	9
2.1	Oblast působnosti stanoviska	9
2.2	Klíčové pojmy	11
2.3	Modely AI v kontextu tohoto stanoviska	11
3	Podstata žádosti	13
3.1	Povaha modelů AI ve vztahu k definici osobních údajů.....	13
3.2	Okolnosti, za nichž lze modely AI považovat za anonymní, a doložení této anonymity	14
3.2.1	Obecné úvahy týkající se anonymizace v daném kontextu	15
3.2.2	Prvky pro vyhodnocení zbytkové pravděpodobnosti identifikace.....	17
3.3	Vhodnost oprávněného zájmu jako právního základu pro zpracování osobních údajů v souvislosti s vývojem a zaváděním modelů AI	19
3.3.1	Obecné připomínky	20
3.3.2	Úvahy o třech krocích posuzování oprávněného zájmu v souvislosti s vývojem a zaváděním modelů AI	21
3.4	Možný dopad protiprávního zpracování při vývoji modelu AI na zákonnost následného zpracování nebo provozu modelu AI	31
3.4.1	Scénář č. 1. Správce protiprávně zpracovává osobní údaje za účelem vývoje modelu, osobní údaje jsou uchovávány v modelu a následně zpracovávány stejným správcem (například v souvislosti se zavedením modelu).....	33
3.4.2	Scénář č. 2. Správce protiprávně zpracovává osobní údaje za účelem vývoje modelu, osobní údaje jsou uchovávány v modelu a zpracovávány jiným správcem v souvislosti se zavedením modelu	33
3.4.3	Scénář č. 3. Správce protiprávně zpracovává osobní údaje za účelem vývoje modelu, poté zajistí, aby byl model anonymizován, a to předtím, než stejný nebo jiný správce zahájí další zpracování osobních údajů v souvislosti se zaváděním	35
4	Závěrečné poznámky	35

Evropský sbor pro ochranu osobních údajů,

s ohledem na článek 63 a čl. 64 odst. 2 nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (dále jen „obecné nařízení o ochraně osobních údajů“),

s ohledem na Dohodu o EHP, a zejména na přílohu XI a protokol 37 k uvedené dohodě ve znění rozhodnutí Smíšeného výboru EHP č. 154/2018 ze dne 6. července 2018¹,

s ohledem na články 10 a 22 svého jednacího řádu,

vzhledem k těmto důvodům:

(1) Hlavní úlohou Evropského sboru pro ochranu osobních údajů (dále jen „**sbor**“ nebo „**EDPB**“) je zajistit jednotné uplatňování obecného nařízení o ochraně osobních údajů v celém Evropském hospodářském prostoru (dále jen „**EHP**“). Čl. 64 odst. 2 obecného nařízení o ochraně osobních údajů stanoví, že kterýkoli dozorový úřad, předseda sboru nebo Komise mohou požádat, aby sbor posoudil jakoukoli záležitost s obecnou působností nebo s účinky ve více než jednom členském státě EHP za účelem získání stanoviska. Účelem tohoto stanoviska je posoudit záležitost s obecnou působností nebo s účinky ve více než jednom členském státě EHP.

(2) Stanovisko sboru bude podle čl. 64 odst. 3 obecného nařízení o ochraně osobních údajů ve spojení s čl. 10 odst. 2 jednacího řádu EDPB přijato do osmi týdnů od okamžiku, kdy předseda a příslušný dozorový úřad rozhodnou, že předložený spis je úplný. Z rozhodnutí předsedy může být tato lhůta s ohledem na složitost dané záležitosti prodloužena o dalších šest týdnů,

PŘIJAL TOTO STANOVISKO:

1 Úvod

1.1 Shrnutí skutečností

1. Dne 4. září 2024 požádal **irský dozorový úřad** (dále též „**žádající dozorový úřad**“) EDPB o vydání stanoviska podle čl. 64 odst. 2 obecného nařízení o ochraně osobních údajů v souvislosti s modely AI a zpracováním osobních údajů (dále jen „**žádost**“).
2. Předsedkyně sboru a irský dozorový úřad uznaly spis za úplný dne 13. září 2024. Následující pracovní den, 16. září 2024, sekretariát EDPB spis zveřejnil. Předsedkyně sboru s ohledem na složitost dané záležitosti rozhodla o prodloužení zákonné lhůty v souladu s čl. 64 odst. 3 obecného nařízení o ochraně osobních údajů a čl. 10 odst. 4 jednacího řádu EDPB.
3. Žádost se týká některých prvků trénování, aktualizace, vývoje a provozu modelů AI, kdy jsou součástí příslušného souboru údajů osobní údaje. Irský dozorový úřad zdůrazňuje, že se žádost týká klíčových otázek, které mají značný dopad na subjekty údajů a správce v EHP, a že v této fázi neexistuje mezi

¹ Pokud se v tomto stanovisku hovoří o „členských státech“, rozumějí se tím „členské státy EHP“. Pokud se v tomto stanovisku hovoří o „Unii“, rozumí se tím „EHP“.

vnitrostátními dozorovými úřady žádný harmonizovaný postoj². Terminologie, která bude použita pro účely tohoto stanoviska, je uvedena v oddílech 2.2 a 2.3 níže.

4. Irský dozorový úřad položil tyto otázky:

Otázka č. 1: Považuje se konečný model AI, který byl vytrénován s použitím osobních údajů, ve všech případech za model, který nesplňuje definici osobních údajů (uvedenou v čl. 4 odst. 1 obecného nařízení o ochraně osobních údajů)?

V případě kladné odpovědi na otázku č. 1:

- i. V jaké fázi operací zpracování vedoucích k vytvoření modelu AI již nejsou zpracovávány osobní údaje?
 - a) Jak lze doložit, že model AI nezpracovává osobní údaje?
- ii. Existují nějaké faktory, které by vedly k tomu, že by provoz konečného modelu AI již nebyl považován za anonymní?
 - a) Pokud ano, jak lze doložit opatření přijatá ke zmírnění, prevenci nebo ochraně před těmito faktory (aby se zajistilo, že model AI nezpracovává osobní údaje)?

V případě záporné odpovědi na otázku č. 1:

- i. Za jakých okolností by mohla nastat taková situace?
 - a) Pokud nastane, jak lze doložit kroky, které byly přijaty k zajištění toho, aby model AI nezpracovával osobní údaje?

Otázka č. 2: Pokud se správce údajů spoléhá na oprávněné zájmy jako na právní základ pro zpracování osobních údajů za účelem vytvoření, aktualizace a/nebo vývoje modelu AI, jak by měl správce údajů doložit vhodnost oprávněných zájmů jako právního základu, a to jak ve vztahu ke zpracování osobních údajů třetí strany, tak údajů první strany?

- i. Jaká hlediska by měl správce zohlednit, aby zajistil, že zájmy subjektů údajů, jejichž osobní údaje jsou zpracovávány, jsou vhodně vyváženy se zájmy správce v souvislosti s:
 - a) údaji třetí strany;
 - b) údaji první strany.

Otázka č. 3: Pokud správce údajů spoléhá na oprávněné zájmy jako právní základ pro zpracování osobních údajů v rámci modelu AI nebo systému AI, jehož je model AI součástí, jak by měl správce údajů ve fázi po vytrénování modelu doložit vhodnost oprávněných zájmů jako právního základu?

Otázka č. 4: Pokud bylo zjištěno, že model AI byl vytvořen, aktualizován nebo vyvinut s použitím protiprávně zpracovávaných osobních údajů, jaký je případný dopad této skutečnosti na zákonnost dalšího nebo následného zpracování nebo provozu modelu AI, ať už samostatně, nebo jako součástí systému AI, pokud:

- i. model AI, ať už samostatně, nebo jako součást systému AI, zpracovává osobní údaje?
- ii. ani model AI sám o sobě, ani model AI jako součást systému AI nezpracovává osobní údaje?

² Žádost, s. 1.

1.2 Přípustnost žádosti o stanovisko podle čl. 64 odst. 2 obecného nařízení o ochraně osobních údajů

5. Čl. 64 odst. 2 obecného nařízení o ochraně osobních údajů stanoví, že kterýkoli dozorový úřad může požádat, aby EDPB posoudil jakoukoli záležitost s obecnou působností nebo s účinky ve více než jednom členském státě za účelem získání stanoviska.
6. Žádající dozorový úřad se obrátil na EDPB s otázkami týkajícími se aspektů ochrany osobních údajů v souvislosti s modely AI. V žádosti bylo uvedeno, že přestože mnoho organizací nyní používá modely AI, včetně velkých jazykových modelů, jejich provoz, trénování a používání vyvolávají „řadu dalekosáhlých obav v oblasti ochrany osobních údajů“³, které „mají dopad na subjekty údajů v celé EU/EHP“⁴.
7. V žádosti se v podstatě vznášejí otázky týkající se i) použití pojmu osobní údaje; ii) zásady zákonnosti, se zvláštním ohledem na právní základ spočívající v oprávněném zájmu, a to v souvislosti s modely AI; jakož i iii) důsledků protiprávního zpracování osobních údajů ve fázi vývoje modelů AI pro následné zpracování nebo provoz modelu.
8. Sbor se proto domnívá, že tato žádost se týká „záležitosti s obecnou působností“ ve smyslu čl. 64 odst. 2 obecného nařízení o ochraně osobních údajů. Tato záležitost se týká zejména výkladu a uplatňování čl. 4 odst. 1, čl. 5 odst. 1 písm. a) a článku 6 obecného nařízení o ochraně osobních údajů v souvislosti se zpracováním osobních údajů při vývoji a zavádění modelů AI. Jak zdůraznil žádající dozorový úřad, uplatnění těchto ustanovení na modely AI vyvolává systémové, abstraktní a nové otázky⁵. Rychlý vývoj a zavádění modelů AI stále více organizacemi vyvolává konkrétní otázky, a jak je uvedeno v žádosti, „EDPB bude mít velký prospěch z toho, pokud dospěje ke společnému postoji k záležitostem uvedeným v této žádosti, neboť tyto záležitosti jsou zásadní pro plánovanou činnost EDPB v krátkodobém a střednědobém horizontu“⁶. Kromě toho technologie umělé inteligence vytvářejí mnoho příležitostí a přinášejí mnoho výhod v celé řadě odvětví a společenských aktivit. Obecné nařízení o ochraně osobních údajů je navíc právním rámcem, který podporuje odpovědné inovace. Z toho vyplývá, že existuje obecný zájem na provedení tohoto posouzení ve formě stanoviska EDPB s cílem zajistit jednotné uplatňování některých ustanovení obecného nařízení o ochraně osobních údajů v souvislosti s modely AI.
9. Alternativní podmínka uvedená v čl. 64 odst. 2 obecného nařízení o ochraně osobních údajů se týká záležitostí „s účinky ve více než jednom členském státě“. EDPB připomíná, že pojem „účinky“ je třeba vykládat *lato sensu* (v širším smyslu), a neomezuje se tedy pouze na právní účinky⁷. Vzhledem k tomu, že stále více modelů AI je vytrénováno a používáno stále větším počtem organizací v EHP, mají tyto modely dopad na velký počet subjektů údajů v celém EHP, z nichž některé již vznesly obavy u svého

³ Žádost, s. 1.

⁴ Tamtéž.

⁵ Žádost, s. 2.

⁶ Žádost, s. 1. Jak je uvedeno v pracovním programu EDPB na období 2024–2025, přijatém dne 8. října 2024, který je k dispozici na adrese https://www.edpb.europa.eu/system/files/2024-10/edpb_work_programme_2024-2025_en.pdf, EDPB plánuje vydat *mimo jiné* pokyny k anonymizaci, pseudonymizaci a scrapingu údajů v souvislosti s generativní AI.

⁷ EDPB, interní dokument 3/2019 o interních pokynech k čl. 64 odst. 2 obecného nařízení o ochraně osobních údajů, přijatý dne 8. října 2019, bod 15, k dispozici na adrese https://www.edpb.europa.eu/system/files/2022-07/internaledpb_document_201903_art64.2_en.pdf.

příslušného dozorového úřadu⁸. EDPB se proto domnívá, že záležitost, kterou předložil žádající dozorový úřad, rovněž splňuje tuto podmínku.

10. Žádost obsahuje písemné odůvodnění týkající se souvislostí a důvodů pro předložení otázek sboru, včetně příslušného právního rámce. Sbor se proto domnívá, že žádost je odůvodněna v souladu s čl. 10 odst. 3 jednacího řádu EDPB.
11. Podle čl. 64 odst. 3⁹ obecného nařízení o ochraně osobních údajů EDPB nevydá stanovisko, pokud již vydal stanovisko ke stejné záležitosti. EDPB nevydal stanovisko ke stejné záležitosti a dosud neposkytl odpovědi na otázky vyplývající ze žádosti.
12. Z těchto důvodů se sbor domnívá, že žádost je přípustná a otázky z ní vyplývající by měly být analyzovány v tomto stanovisku (dále jen „**stanovisko**“) přijatém podle čl. 64 odst. 2 obecného nařízení o ochraně osobních údajů.

2 Oblast působnosti a klíčové pojmy

2.1 Oblast působnosti stanoviska

13. Sbor souhlasí s žádajícím dozorovým úřadem, že z hlediska ochrany osobních údajů vyvolává vývoj a zavádění modelů AI zásadní otázky týkající se ochrany údajů. Otázky se týkají zejména toho: i) kdy a jak lze model AI považovat za „anonymní“ (otázka č. 1 žádosti); ii) jak mohou správci údajů doložit vhodnost oprávněného zájmu jako právního základu ve fázi vývoje (otázka č. 2 žádosti) a ve fázi zavádění (otázka č. 3 žádosti) a iii) zda má protiprávní zpracování osobních údajů ve fázi vývoje důsledky pro zákonnost následného zpracování nebo provozu modelu AI (otázka č. 4 žádosti).
14. EDPB připomíná, že dozorové úřady jsou odpovědné za monitorování uplatňování obecného nařízení o ochraně osobních údajů a měly by přispívat k jeho jednotnému uplatňování v celé Unii¹⁰. Je proto v pravomoci dozorových úřadů prozkoumat konkrétní modely AI a v tomto ohledu provádět posouzení jednotlivých případů.
15. Toto stanovisko poskytuje příslušným dozorovým úřadům rámec pro posouzení konkrétních případů, v nichž by vyvstaly (některé) otázky uvedené v žádosti. Neklade si za cíl být vyčerpávající, ale spíše uvést obecné úvahy o výkladu příslušných ustanovení, které by měly příslušné dozorové úřady při využívání svých vyšetřovacích pravomocí co nejvíce zohlednit. Přestože je toto stanovisko určeno příslušným dozorovým úřadům a týká se jejich činností a pravomocí, nejsou jím dotčeny povinnosti správců a zpracovatelů podle obecného nařízení o ochraně osobních údajů. Zejména podle zásady odpovědnosti zakotvené v čl. 5 odst. 2 obecného nařízení o ochraně osobních údajů jsou správci odpovědní za dodržování všech zásad týkajících se zpracování osobních údajů a musí být schopni toto dodržování doložit.
16. Pro některé případy může být ve stanovisku uvedeno několik příkladů, ale vzhledem k širokému záběru otázek obsažených v žádosti, jakož i k různým typům modelů AI, které jsou předmětem žádosti, nebudou v tomto stanovisku rozebrány všechny možné scénáře. Technologie spojené s modely AI podléhají rychlému vývoji, a proto by úvahy EDPB v tomto stanovisku měly být vykládány s ohledem na tuto skutečnost.

⁸ Žádost, s. 1–2.

⁹ Čl. 64 odst. 3 obecného nařízení o ochraně osobních údajů a čl. 10 odst. 4 jednacího řádu EDPB.

¹⁰ Čl. 51 odst. 1 a 2 obecného nařízení o ochraně osobních údajů.

17. **V tomto stanovisku nejsou analyzována níže uvedená ustanovení, která mohou stále hrát důležitou úlohu při posuzování požadavků na ochranu osobních údajů vztahujících se na modely AI:**

- **Zpracování zvláštních kategorií údajů:** EDPB připomíná zákaz stanovený v čl. 9 odst. 1 obecného nařízení o ochraně osobních údajů, pokud jde o zpracování zvláštních kategorií údajů, a omezené výjimky stanovené v čl. 9 odst. 2 obecného nařízení o ochraně osobních údajů¹¹. V tomto ohledu Soudní dvůr Evropské unie (dále jen „SDEU“) dále objasnil, že „*v případě, kdy je soubor údajů, který obsahuje jak citlivé, tak necitlivé údaje, [...] shromažďován jako celek, aniž mohou být údaje v okamžiku tohoto shromažďování od sebe odděleny, musí být zpracování tohoto souboru údajů považováno za zakázané ve smyslu čl. 9 odst. 1 obecného nařízení o ochraně osobních údajů, pokud obsahuje alespoň jeden citlivý údaj a nepoužije se žádná z výjimek uvedených v čl. 9 odst. 2 tohoto nařízení*“¹². Kromě toho Soudní dvůr EU rovněž zdůraznil, že ¹³ „*pro účely uplatnění výjimky stanovené v čl. 9 odst. 2 písm. e) obecného nařízení o ochraně osobních údajů je třeba ověřit, zda subjekt údajů zamýšlel výslovně a jednoznačným potvrzujícím úkonem zpřístupnit předmětné osobní údaje široké veřejnosti*“. Tyto úvahy by měly být zohledněny, pokud zpracování osobních údajů v souvislosti s modely AI zahrnuje zvláštní kategorie údajů.
- **Automatizované rozhodování, včetně profilování:** Operace zpracování prováděné v rámci modelů AI mohou spadat do oblasti působnosti článku 22 obecného nařízení o ochraně osobních údajů, který správcům ukládá další povinnosti a subjektům údajů poskytuje další záruky. EDPB v této souvislosti připomíná své pokyny k automatizovanému individuálnímu rozhodování a profilování pro účely nařízení 2016/679¹⁴.
- **Slučitelnost účelů:** Čl. 6 odst. 4 obecného nařízení o ochraně osobních údajů stanoví pro určité právní základy kritéria, která správce zohlední v zájmu zjištění toho, zda je zpracování pro jiný účel slučitelné s účelem, pro který byly osobní údaje původně shromážděny. Toto ustanovení může být relevantní v souvislosti s vývojem a zaváděním modelů AI a jeho použitelnost by měly posoudit dozorové úřady.
- **Posouzení vlivu na ochranu osobních údajů** (článek 35 obecného nařízení o ochraně osobních údajů): Posouzení vlivu na ochranu osobních údajů jsou důležitým prvkem odpovědnosti v případech, kdy zpracování v souvislosti s modely AI bude mít za následek vysoké riziko pro práva a svobody fyzických osob¹⁵.

¹¹ Viz také zpráva EDPB o práci vykonané pracovní skupinou ChatGPT, přijatá dne 23. května 2024, bod 18: „Pokud jde o zpracování zvláštních kategorií osobních údajů, musí se navíc uplatnit jedna z výjimek uvedených v čl. 9 odst. 2, aby bylo zpracování zákonné. V zásadě může být jednou z těchto výjimek čl. 9 odst. 2 písm. e) obecného nařízení o ochraně osobních údajů. Samotná skutečnost, že osobní údaje jsou veřejně přístupné, však neznamená, že „osobní údaje byly tímto uživatelem zjevně zveřejněny“ [...]“.

¹² Rozsudek SDEU ze dne 4. července 2023, věc C-252/21, *Meta proti Bundeskartellamt* (ECLI:EU:C:2023:537), bod 89.

¹³ Rozsudek SDEU ze dne 4. července 2023, věc C-252/21, *Meta proti Bundeskartellamt* (ECLI:EU:C:2023:537), bod 77.

¹⁴ Pracovní skupina zřízená podle článku 29, pokyny k automatizovanému individuálnímu rozhodování a profilování pro účely nařízení 2016/679 ve znění naposledy revidovaném a přijatém dne 6. února 2018, schválené EDPB dne 25. května 2018. Viz rovněž rozsudek SDEU ze dne 7. prosince 2023, věc C-634/21, *SCHUFA Holding a další* (ECLI:EU:C:2023:957).

¹⁵ Pracovní skupina zřízená podle článku 29, pokyny pro posouzení vlivu na ochranu údajů a stanovení, zda „je pravděpodobné, že zpracování osobních údajů bude mít za následek vysoké riziko“ pro účely nařízení 2016/679, přijaté dne 4. října 2017 v aktualizovaném znění, schválené EDPB dne 25. května 2018.

- **Zásada záměrné ochrany osobních údajů** (čl. 25 odst. 1 obecného nařízení o ochraně osobních údajů): Záměrná ochrana osobních údajů je základní zárukou, kterou by měly dozorové úřady posoudit v souvislosti s vývojem a zaváděním modelu AI.

2.2 Klíčové pojmy

18. Jako předběžnou poznámku by EDPB rád poskytl vysvětlení k terminologii a pojmům, které používá v tomto stanovisku, a to pouze pro účely tohoto stanoviska:

- „**Údaji první strany**“ se rozumí osobní údaje, které správce shromáždil od subjektů údajů.
- „**Údaji třetí strany**“ se rozumí osobní údaje, které správci nezískali od subjektů údajů, ale shromáždili je nebo obdrželi od třetí strany, například od zprostředkovatele údajů nebo je shromáždili prostřednictvím web scrapingu.
- „**Web scrapingem**“ se rozumí běžně používaná metoda shromažďování informací z veřejně dostupných on-line zdrojů. Informace, které byly získány například ze služeb, jako jsou sdělovací prostředky, sociální sítě, diskuse na fórech a osobní internetové stránky, mohou obsahovat osobní údaje.
- V žádosti se zmiňuje „**životní cyklus**“ modelů AI, jakož i různé fáze týkající se mimo jiné „vytváření“, „vývoje“, „trénování“, „aktualizace“, „dolaďování“, „provozu“ nebo „fáze po vytrénování“ modelů AI. EDPB uznává, že v závislosti na okolnostech mohou tyto fáze probíhat v rámci vývoje a zavádění modelů AI a mohou zahrnovat zpracování osobních údajů pro různé účely zpracování. Pro potřeby tohoto stanoviska však EDPB považuje za důležité zjednodušit kategorizaci fází, které pravděpodobně nastanou. EDPB proto pro účely tohoto stanoviska odkazuje na „**fázi vývoje**“ a na „**fázi zavádění**“. Vývoj modelu AI zahrnuje všechny fáze před jakýmkoli zavedením modelu AI a zahrnuje mimo jiné vývoj programu, shromáždění trénovacích osobních údajů, předběžné zpracování trénovacích osobních údajů a trénování. Zavedení modelu AI zahrnuje všechny fáze související s používáním modelu AI a může zahrnovat jakékoli operace provedené po fázi vývoje. EDPB si je stále vědom různých případů použití a jejich možných důsledků, pokud jde o zpracování osobních údajů. Dozorové úřady by tudíž měly zvážit, zda jsou připomínky uvedené v tomto stanovisku relevantní pro zpracování, které posuzují.
- EDPB rovněž zdůrazňuje, že v případě potřeby se pojem „**trénování**“ vztahuje na tu část fáze vývoje, kdy se modely AI učí na základě dat plnit svůj zamýšlený úkol (jak je vysvětleno v následujícím oddíle tohoto stanoviska).
- Koncepce a rozsah **modelů AI**, jak je chápe EDPB pro účely tohoto stanoviska, jsou dále upřesněny v následujícím specializovaném oddíle.

2.3 Modely AI v kontextu tohoto stanoviska

19. V aktu EU o umělé inteligenci (dále jen „**akt o AI**“)¹⁶ je „systém AI“ definován jako „*strojový systém navrhovaný tak, aby po zavedení fungoval s různými úrovněmi autonomie a který po zavedení může vykazovat adaptabilitu a který za explicitními nebo implicitními účely z obdržených vstupů odvozuje, jak generovat výstupy, jako jsou predikce, obsah, doporučení nebo rozhodnutí, které mohou ovlivnit fyzická*

¹⁶ Nařízení Evropského parlamentu a Rady (EU) 2024/1689 ze dne 13. června 2024, kterým se stanoví harmonizovaná pravidla pro umělou inteligenci a mění nařízení (ES) č. 300/2008, (EU) č. 167/2013, (EU) č. 168/2013, (EU) 2018/858, (EU) 2018/1139 a (EU) 2019/2144 a směrnice 2014/90/EU, (EU) 2016/797 a (EU) 2020/1828 (akt o umělé inteligenci).

nebo virtuální prostředí“¹⁷. Ve 12. bodě odůvodnění aktu o umělé inteligenci je pojem „systém AI“ vysvětlen podrobněji. Jednou z klíčových vlastností systémů AI je podle tohoto ustanovení jejich schopnost odvozování. Mezi techniky, které umožňují odvozování při současném budování systému AI, patří strojové učení a přístupy založené na logice a poznatcích.

20. „Modely AI“ jsou na druhé straně v aktu o AI definovány pouze nepřímo: „Ačkoli jsou modely AI základními součástmi systémů AI, nepředstavují samy o sobě systémy AI. Modely AI vyžadují doplnění dalších součástí, jako je například uživatelské rozhraní, aby se z nich staly systémy AI. Modely AI jsou obvykle začleněny do systémů AI a tvoří jejich součást.“¹⁸
21. EDPB chápe, že definice modelu AI navržená v žádosti je užší než definice podle aktu o AI, neboť se v ní o „modelu AI“ hovoří jako o modelu „zahrnujícím produkt, který je výsledkem trénovacích mechanismů, jež jsou aplikovány na soubor trénovacích dat, v kontextu umělé inteligence, strojového učení, hlubokého učení nebo jiných souvisejících kontextů zpracování“, přičemž je upřesněno, že „pojem se vztahuje na modely AI, které jsou určeny k dalšímu trénování, doladování a/nebo vývoji, jakož i na modely AI, které k takovýmto postupům určeny nejsou.“¹⁹
22. Na základě toho přijal EDPB toto stanovisko s tím, že systém AI bude při plnění zamýšleného cíle spoléhat na model AI, který bude začleněn do širšího rámce (např. systém AI pro služby zákazníkům může využívat model AI vytrénovaný na základě historických dat z rozhovorů k poskytování odpovědí na dotazy uživatelů).
23. Kromě toho jsou pro toto stanovisko relevantní modely AI (dále též „**modely**“) vyvinuté v rámci procesu trénování. Tento proces trénování je součástí fáze vývoje, kdy se modely učí z dat, jak plnit úkoly, k nimž jsou určeny. Proces trénování proto vyžaduje soubor údajů, z něhož model identifikuje určité vzorce a „učí se“ je. V těchto případech bude model používat různé techniky k vytvoření reprezentace znalostí extrahovaných z trénovacího souboru údajů. To platí zejména v případě strojového učení.
24. V praxi je každý model AI algoritmem, jehož fungování je určeno souborem prvků. Například modely hlubokého učení mají často formu neuronové sítě s více vrstvami sestávajícími z uzlů propojených hranami, které mají váhy, jež jsou během trénování upraveny tak, aby se naučily vztahy mezi vstupy a výstupy. Charakteristickými rysy jednoduchého modelu hlubokého učení by byly: i) typ a velikost každé vrstvy; ii) váha připisovaná každé hraně (někdy označovaná jako „parametry“); iii) aktivační funkce²⁰ mezi vrstvami a případně iv) jiné operace, které se mohou mezi vrstvami uskutečnit. Například při trénování jednoduchého modelu hlubokého učení pro klasifikaci obrázků budou vstupy („**obrázkové pixely**“) přiřazeny k výstupům a váhy mohou být upraveny tak, aby ve většině případů poskytovaly správný výstup.
25. Dalšími příklady modelů hlubokého učení jsou velké jazykové modely a generativní AI, které se používají např. pro generování obsahu připomínajícího lidský výstup a vytváření nových dat.
26. **Na základě výše uvedených úvah a v souladu s žádostí se oblast působnosti tohoto stanoviska vztahuje pouze na podmnožinu modelů AI, které jsou výsledkem trénování těchto modelů na základě osobních údajů.**

¹⁷ Viz čl. 3 bod 1 aktu o AI.

¹⁸ 97. bod odůvodnění aktu o AI.

¹⁹ Žádost, s. 3.

²⁰ Tj. funkce, které na základě vstupů a vah vypočítávají výstup neuronového uzlu, který bude poté odeslán do další vrstvy neuronové sítě.

3 Podstata žádosti

3.1 Povaha modelů AI ve vztahu k definici osobních údajů

27. Čl. 4 odst. 1 obecného nařízení o ochraně osobních údajů definuje osobní údaje jako „*veškeré informace o identifikované nebo identifikovatelné fyzické osobě*“ (tj. subjektu údajů). Kromě toho 26. bod odůvodnění obecného nařízení o ochraně osobních údajů stanoví, že zásady ochrany údajů by se neměly vztahovat na anonymní informace, totiž informace, které se netýkají identifikované či identifikovatelné fyzické osoby, s přihlédnutím ke „*všem prostředkům [...], o nichž lze rozumně předpokládat, že je správce nebo jiná osoba použije*“. Patří sem: i) údaje, které se nikdy nevztahovaly k identifikované nebo identifikovatelné osobě; a ii) osobní údaje anonymizované tak, že subjekt údajů není nebo již přestal být identifikovatelným.
28. V souladu s tím lze na otázku č. 1²¹ žádosti odpovědět analýzou, zda by model AI, který je výsledkem trénování zahrnujícího zpracování osobních údajů, měl být ve všech případech považován za anonymní. Na základě formulace otázky bude EDPB v tomto oddíle odkazovat na proces „trénování“ modelu AI.
29. V první řadě by EDPB rád uvedl následující obecné úvahy. Modely AI, bez ohledu na to, zda jsou vytrénovány na základě osobních údajů, či nikoli, jsou obvykle navrženy tak, aby vytvářely prognózy nebo vyvozovaly závěry, tj. jsou navrženy k odvozování. Kromě toho jsou modely AI vytrénované na základě osobních údajů často navrženy tak, aby odvozovaly závěry o jiných osobách než o těch, jejichž osobní údaje byly použity ke trénování modelu AI. Některé modely AI jsou však konkrétně navrženy tak, aby poskytovaly osobní údaje týkající se fyzických osob, jejichž osobní údaje byly použity ke trénování modelu, nebo nějakým způsobem k jejich zpřístupnění. V těchto případech budou takové modely AI neodmyslitelně (a obvykle nutně) zahrnovat informace týkající se identifikované nebo identifikovatelné fyzické osoby, a budou tedy zahrnovat zpracování osobních údajů. Proto tyto druhy modelů AI nelze považovat za anonymní. Bude tomu tak například v případě i) generativního modelu vyladěného na základě hlasových nahrávek jednotlivce tak, aby napodoboval jeho hlas; nebo ii) jakéhokoli modelu navrženého tak, aby na výzvu k poskytnutí informací o konkrétní osobě odpovídal osobními údaji získanými na základě trénování.
30. Na základě výše uvedených úvah se EDPB v odpovědi na otázku č. 1 žádosti zaměřuje na situaci modelů AI, které nejsou určeny k poskytování osobních údajů souvisejících s trénovacími daty.
31. EDPB se domnívá, že i když model AI nebyl záměrně navržen tak, aby z trénovacích dat vytvářel informace týkající se identifikované nebo identifikovatelné fyzické osoby, mohou informace z trénovacího souboru dat, včetně osobních údajů, být „absorbovány“ v parametrech modelu, konkrétně reprezentovány prostřednictvím matematických objektů. Mohou se lišit od původních trénovacích dat, ale mohou stále uchovávat původní informace o těchto datech, které mohou být nakonec přímo či nepřímo extrahovatelné z modelu nebo z něj mohou být získávány jinak. Kdykoli lze z modelu AI získat informace týkající se identifikovaných nebo identifikovatelných fyzických osob, jejichž osobní údaje byly použity k trénování modelu, a to prostředky, o nichž lze rozumně předpokládat, že budou použity, lze dojít k závěru, že takový model není anonymní.
32. V tomto ohledu se v žádosti uvádí, že „*ve stávajících výzkumných publikacích se poukazuje na určitá případná zranitelná místa, která mohou existovat v modelech AI a která by mohla vést ke zpracování*

²¹ „Považuje se konečný model AI, který byl vytrénován s použitím osobních údajů, ve všech případech za model, který nesplňuje definici osobních údajů (uvedenou v čl. 4 odst. 1 obecného nařízení o ochraně osobních údajů)?“.

osobních údajů²², jakož i ke zpracování osobních údajů, které může pokračovat, pokud jsou modely zavedeny pro použití s jinými údaji, a to buď prostřednictvím aplikačních programovacích rozhraní („API“) nebo rozhraní pro zadávání dotazů (tzv. prompt interface)²³.

33. Obdobně platí, že obzvláště dynamický je výzkum v oblasti extrakce trénovacích dat²⁴. Vyplývá z něj, že v některých případech je možné použít prostředky, o nichž lze rozumně předpokládat, že budou extrahovat osobní údaje z některých modelů AI, nebo jednoduše náhodně získávat osobní údaje prostřednictvím interakcí s modelem AI (například jako součást systému AI). Setrvalé výzkumné úsilí v tomto oboru pomůže dále posoudit zbytková rizika regurgitace²⁵ a extrakce osobních údajů v každém jednotlivém případě.
34. **Na základě výše uvedených úvah se EDPB domnívá, že modely AI trénované na osobních údajích nelze ve všech případech považovat za anonymní. Místo toho by mělo být na základě konkrétních kritérií v každém jednotlivém případě posouzeno, zda je model AI anonymní.**

3.2 Okolnosti, za nichž lze modely AI považovat za anonymní, a doložení této anonymity

35. Pokud jde o otázku č. 1 žádosti²⁶, EDPB se žádá, aby objasnil okolnosti, za nichž lze model AI, který byl trénován s použitím osobních údajů, považovat za anonymní. Pokud jde o otázku č. 1 písm. i) bod a) žádosti²⁷, EDPB se žádá, aby objasnil, které důkazy a/nebo dokumentaci by měly dozorové úřady zohlednit při posuzování, zda je model AI anonymní.

²² Např. útoky založené na odvozování členství ([OWASP](#)) a útoky založené na invertování modelu ([OWASP](#) a [Veale a kol.](#), 2018).

²³ Žádost, s. 1–2.

²⁴ V tomto ohledu viz například: i) Veale M., Binns R., Edwards L., 2018, *Algorithms that remember: model inversion attacks and data protection law* (Algoritmy, které si pamatují: útoky založené na invertování modelu a právní předpisy o ochraně údajů). Phil. Trans. R. Soc. A 376: 20180083, k dispozici na adrese <http://dx.doi.org/10.1098/rsta.2018.0083>; ii) Brown H., Lee K., Mireshghallah F., Shokri R., a Tramèr F., *What Does it Mean for a Language Model to Preserve Privacy?* (Co znamená zachovávání soukromí pro jazykový model?), 2022, ACM Digital Library, FAccT '22, 20. června 2022, Soul, Korejská republika, k dispozici na adrese <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* (Nepřátelské strojové učení: taxonomie a terminologie útoků a zmírňování), leden 2024, National Institute of Standards and Technology, k dispozici na adrese <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* (Extrakce trénovacích dat z velkých jazykových modelů), arXiv:2012.07805v2 [cs.CR], 15. června 2021, k dispozici na adrese <https://arxiv.org/pdf/2012.07805>; v) Fredrikson M., Jha S., Ristenpart T., *Model Inversion Attacks that Exploit Confidence Information and Basic Countermeasures* (Útoky založené na invertování modelu, které využívají důvěrné informace, a základní protiopatření), ACM Digital Library, 12. října 2015, k dispozici na adrese <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* (Odhalovač tajemství: útoky založené na invertování generativního modelu namířené proti hlubokým neuronovým sítím), arXiv:1911.07135v2 [cs.LG], 18. dubna 2020, k dispozici na adrese <https://arxiv.org/pdf/1911.07135>.

²⁵ U systému AI založeného na generativní AI znamená regurgitace situaci, kdy výstupy přímo souvisejí s trénovacími daty.

²⁶ „Za jakých okolností by mohla nastat taková situace?“.

²⁷ „Pokud nastane, jak lze doložit kroky, které byly přijaty k zajištění toho, aby model AI nezpracovával osobní údaje?“.

3.2.1 Obecné úvahy týkající se anonymizace v daném kontextu

36. Použití výrazu „veškeré informace“ v definici „osobních údajů“ v čl. 4 odst. 1 obecného nařízení o ochraně osobních údajů odráží cíl přidělit tomuto pojmu široký rozsah, který zahrnuje všechny druhy informací, pokud jde o informace o subjektu údajů, který je nebo může být přímo či nepřímo identifikován.
37. Informace se mohou týkat fyzické osoby, i když jsou technicky uspořádány nebo zakódovány (například pouze ve strojově čitelném formátu, ať již proprietárním, nebo otevřeným) způsobem, ze kterého není vztah s touto fyzickou osobou okamžitě zjevný. V takových případech lze pro snadnou identifikaci, rozpoznání a extrakci konkrétních údajů použít softwarové aplikace. To platí zejména pro modely AI, kde parametry představují statistické vztahy mezi trénovacími daty a kde může být možné extrahovat přesné nebo nepřesné (jelikož jsou statisticky odvozené) osobní údaje, a to buď přímo ze vztahů mezi daty obsaženými v modelu, nebo vyhledáváním v tomto modelu.
38. Vzhledem k tomu, že modely AI obvykle neobsahují záznamy, které lze přímo izolovat nebo propojit, ale naopak parametry představující pravděpodobnostní vztahy mezi daty obsaženými v modelu, může být v reálných scénářích možné z modelu odvodit²⁸ informace, jako je členství. Proto, aby dozorový

²⁸ i) Carlini N., Chien S., Nasr M., Song S., Terzis A., Tramer F., *Membership Inference Attacks From First Principles* (Útoky založené na odvozování členství od prvních zásad), arXiv:2112.03570, k dispozici na adrese <https://arxiv.org/abs/2112.03570>;

ii) Crețu A.M., Guépin F. a De Montjoye Y.A., *Correlation inference attacks against machine learning models* (Útoky založené na odvozování korelace zaměřené proti modelům strojového učení). Sci. Adv.10, eadj9260(2024). DOI:10.1126/sciadv.adj9260, k dispozici na adrese <https://www.science.org/doi/10.1126/sciadv.adj9260>;

iii) Dana L., Pydi M. S., Chevalere Y., *Memorization in Attention-only Transformers* (Zapamatování u transformátorů využívajících pouze pozornost) arXiv:2411.10115v1 [cs.AI], 15. listopadu 2024, k dispozici na adrese <https://arxiv.org/abs/2411.10115>;

iv) Gehrke M., Liebenow J., Mohammadi E. a Braun T. a kol. *Lifting in Support of Privacy-Preserving Probabilistic Inference* (Zrušení na podporu pravděpodobnostního odvozování se zachováním soukromí). Künstl Intell, 13. června 2024, k dispozici na adrese <https://doi.org/10.1007/s13218-024-00851-y>;

v) Hu H., *Membership Inference Attacks and Defenses on Machine Learning Models Literature* (Odborná literatura o útocích na modely strojového učení založených na odvozování členství a o obraně před nimi), k dispozici na adrese <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., a Lee K., *Scalable Extraction of Training Data from (Production) Language Models* (Škálovatelná extrakce trénovacích dat z (produkčních) jazykových modelů), arXiv:2311.17035, 28. listopadu 2023, k dispozici na adrese <https://arxiv.org/abs/2311.17035>;

vii) Shokri R., Stronati M., Song C., Shmatikov V., *Membership Inference Attacks against Machine Learning Models* (Útoky založené na odvozování členství proti modelům strojového učení) arXiv:1610.05820v2 [cs.CR], 31. března 2017, k dispozici na adrese <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* (Více než jen zapamatování: porušování ochrany soukromí prostřednictvím odvozování v případě velkých jazykových modelů), arXiv:2310.07298v2, 6. května 2024, k dispozici na adrese <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* (Útoky založené na odvozování v rámci strojového učení jako služby: taxonomie, přezkum a slibný vývoj) arXiv:2406.02027v1 [cs.LG], 27. června 2024, k dispozici na adrese <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* (Útoky založené na odvozování členství nemohou dokázat, že model byl trénován na vašich údajích) arXiv:2409.19798v1, [cs.LG], 29. září 2024, k dispozici na adrese <https://arxiv.org/abs/2409.19798>;

xi) Zhou Z., Xiang J., Chen C., a Su S., *Quantifying and Analyzing Entity-Level Memorization in Large Language Models* (Kvantifikace a analýza zapamatování na úrovni subjektů u velkých jazykových modelů), arXiv:2308.15727v2 [cs.CL], 5. listopadu 2023, k dispozici na adrese <https://arxiv.org/abs/2308.15727>.

úřad mohl souhlasit se správcem, že daný model AI lze považovat za anonymní, měl by přinejmenším ověřit, zda obdržel dostatečné důkazy, že přiměřenými prostředky: i) z modelu nelze extrahovat osobní údaje týkající se trénovacích dat²⁹ a ii) žádný výstup vytvořený při vyhledávání v modelu se netýká subjektů údajů, jejichž osobní údaje byly použity k trénování modelu.

39. Při posuzování toho, zda jsou tyto podmínky splněny, by měly dozorové úřady zvážit tři prvky.
40. Zaprvé by dozorové úřady měly zvážit prvky uvedené v nejnovějších stanoviscích pracovní skupiny zřízené podle článku 29 a/nebo v pokynech EDPB k dané věci. Pokud jde o anonymizaci k datu vydání tohoto stanoviska, dozorové úřady by měly zvážit prvky uvedené ve stanovisku pracovní skupiny zřízené podle článku 29 č. 5/2014 k technikám anonymizace (dále jen „**stanovisko pracovní skupiny zřízené podle článku 29 č. 5/2014**“), v němž se uvádí, že pokud nelze vyčlenit jednotlivé osoby a nelze propojit a dedukovat informace z údajně anonymního souboru údajů, mohou být údaje považovány za anonymní³⁰. Rovněž se zde uvádí, že „[v]ždy, když návrh nesplňuje některé z kritérií, mělo by být provedeno pečlivé posouzení rizika identifikace“³¹. **Vzhledem k výše uvedené pravděpodobnosti extrakce údajů a odvozování se EDPB domnívá, že modely AI budou velmi pravděpodobně vyžadovat takto důkladné hodnocení rizik identifikace.**
41. Zadruhé by toto posouzení mělo být provedeno s přihlédnutím ke „všem prostředkům, o nichž lze rozumně předpokládat, že je správce nebo jiná osoba použije“ k identifikaci fyzických osob³², a určení těchto prostředků by mělo být založeno na objektivních faktorech, jak je vysvětleno ve 26. bodě odůvodnění obecného nařízení o ochraně osobních údajů. Tyto faktory mohou zahrnovat:
- a. vlastnosti samotných trénovacích dat, model AI a postup trénování³³;
 - b. kontext, v němž je model AI zveřejněn a/nebo zpracováván³⁴;
 - c. další informace, které by umožnily identifikaci a které mohou být dané osobě k dispozici;
 - d. náklady a čas, které by daná osoba potřebovala k získání těchto dalších informací (v případě, že tyto informace již nemá k dispozici)³⁵; a
 - e. technologie dostupné v době zpracování, jakož i technologický rozvoj³⁶.
42. Zatřetí by dozorové úřady měly zvážit, zda správci posoudili riziko identifikace ze strany správce a různých typů „jiných osob“, včetně nezamýšlených třetích stran, které mají přístup k modelu AI, rovněž s přihlédnutím k tomu, zda je lze rozumně považovat za schopné získat přístup k dotčeným údajům nebo je zpracovávat.
43. **Souhrnně se tedy EDPB domnívá, že aby mohl být model AI považován za anonymní, měla by být při použití přiměřených prostředků jak i) pravděpodobnost přímé (včetně pravděpodobnostní) extrakce osobních údajů týkajících se osob, jejichž osobní údaje byly použity ke trénování modelu, tak ii) pravděpodobnost extrakce, ať už úmyslné, či neúmyslné, takových osobních údajů na základě dotazů**

²⁹ Extrakce údajů zahrnuje zejména případ, kdy jsou osobní údaje odvozeny ze samotného modelu AI, a to bez rozhraní pro vyhledávání nebo jen s omezeným rozhraním pro vyhledávání.

³⁰ Stanovisko pracovní skupiny zřízené podle článku 29 č. 5/2014, s. 24.

³¹ Stanovisko pracovní skupiny zřízené podle článku 29 č. 5/2014, s. 24.

³² Rozsudek SDEU ze dne 19. října 2016, věc C-582/14, *Breyer proti Bundesrepublik Deutschland* (ECLI:EU:C:2016:779), bod 43.

³³ To zahrnuje charakteristiky, jako je jedinečnost záznamů v trénovacích datech, přesnost informací, agregace, randomizace a zejména to, jak tyto záznamy ovlivňují zranitelnost vůči identifikaci.

³⁴ To zahrnuje kontextové prvky, jako je omezení přístupu pouze na některé osoby a právní záruky.

³⁵ Rozsudek SDEU ze dne 7. března 2024, věc C-479/22 P, *OC proti Evropské komisi* (ECLI:EU:C:2024:215), bod 50.

³⁶ Rozsudek SDEU ze dne 7. března 2024, věc C-479/22 P, *OC proti Evropské komisi* (ECLI:EU:C:2024:215), bod 50.

zanedbatelná³⁷ pro jakýkoli subjekt údajů. Dozorové úřady by měly standardně vzít v úvahu, že modely AI budou pravděpodobně vyžadovat důkladné hodnocení pravděpodobnosti identifikace, aby bylo možné dospět k závěru o jejich možné anonymní povaze. Tato pravděpodobnost by měla být posouzena s ohledem na „všechny prostředky, o nichž lze rozumně předpokládat, že je správce nebo jiná osoba použije“, přičemž by se mělo rovněž zvážit nezamýšlené (opětovné) použití nebo zveřejnění modelu.

3.2.2 Prvky pro vyhodnocení zbytkové pravděpodobnosti identifikace

44. I když mohou být jak ve fázi vývoje, tak ve fázi zavádění přijata opatření, aby se snížila pravděpodobnost získání osobních údajů z modelu AI, měl by se v rámci hodnocení anonymity modelu AI rovněž zvážit přímý přístup k tomuto modelu.
45. Kromě toho by dozorové úřady měly v jednotlivých případech posoudit, zda jsou opatření zavedená správcem k zajištění a doložení anonymity modelu AI vhodná a účinná.
46. Závěr posouzení dozorového úřadu se může lišit zejména u veřejně dostupného modelu AI, který je přístupný neznámému počtu osob s neznámou škálou metod zkoušení a extrakce osobních údajů, a interního modelu AI, který je přístupný pouze zaměstnancům. Zatímco v obou případech by dozorové úřady měly ověřit, zda správci splnili svou povinnost odpovědnosti podle čl. 5 odst. 2 a článku 24 obecného nařízení o ochraně osobních údajů, „prostředky, o nichž lze rozumně předpokládat, že je použije“ jiné osoby, mohou mít dopad na rozsah a povahu možných scénářů, které je třeba zvážit. Proto mohou dozorové úřady v závislosti na kontextu vývoje a zavádění modelu zvážit různé úrovně testování a odolnosti vůči útokům.
47. V tomto ohledu EDPB níže uvádí nepreskriptivní a demonstrativní výčet možných prvků, které mohou dozorové úřady zvážit při posuzování tvrzení správce o anonymitě. Patrně jsou možné i jiné přístupy, pokud nabízejí rovnocennou úroveň ochrany, zejména s ohledem na nejmodernější techniku.
48. Přítomnost nebo nepřítomnost níže uvedených prvků není pro posouzení anonymity modelu AI rozhodujícím kritériem.

3.2.2.1 Návrh modelu AI

49. Pokud jde o návrh modelu AI, dozorové úřady by měly vyhodnotit přístupy správců během fáze vývoje. V tomto ohledu je třeba zvážit uplatňování a účinnost čtyř klíčových oblastí (uvedených níže).

Výběr zdrojů

50. První oblast hodnocení zahrnuje zkoumání výběru zdrojů použitých pro trénování modelu AI. V rámci tohoto hodnocení by dozorové úřady měly vyhodnotit všechny kroky, které vývojáři podnikli, aby se vyhnuli shromažďování osobních údajů nebo je omezili, mimo jiné včetně i) vhodnosti kritérií výběru; ii) relevance a přiměřenosti vybraných zdrojů s ohledem na zamýšlený účel (zamýšlené účely) a iii) toho, zda byly vyloučeny nevhodné zdroje.

Příprava a minimalizace údajů

51. Druhá oblast hodnocení se týká přípravy údajů pro fázi trénování. Dozorové úřady by měly zkoumat zejména: i) zda bylo zváženo použití anonymních a/nebo osobních údajů, které byly pseudonymizovány; a ii) v případě, že bylo rozhodnuto k tomuto opatření nepřikročit, důvody tohoto rozhodnutí s přihlédnutím k zamýšlenému účelu; iii) strategie a techniky minimalizace údajů použité

³⁷ Rozsudek SDEU ze dne 19. října 2016, věc C-582/14, *Breyer proti Bundesrepublik Deutschland* (ECLI:EU:C:2016:779), bod 46, a rozsudek SDEU ze dne 7. března 2024, věc C-479/22 P, *OC proti Evropské komisi* (ECLI:EU:C:2024:215), bod 51.

k omezení objemu osobních údajů zahrnutých do procesu trénování a iv) veškeré procesy filtrování údajů zavedené před trénováním modelu, jejichž cílem je odstranit irelevantní osobní údaje.

Metodická rozhodnutí týkající se trénování

52. Třetí oblast hodnocení se týká výběru spolehlivých metod při vývoji modelů AI. Dozorové úřady by měly posoudit metodická rozhodnutí, která mohou významně snížit nebo vyloučit identifikovatelnost, mimo jiné včetně toho: i) zda tato metodika využívá regularizační metody ke zlepšení generalizace modelu a omezení nadměrného přizpůsobování a především ii) zda správce zavedl vhodné a účinné techniky pro zachování soukromí (např. diferenciální soukromí).

Opatření týkající se výstupů modelu

53. Poslední oblast hodnocení se týká veškerých metod nebo opatření přidanych do samotného modelu AI, které nemusí mít vliv na riziko přímé extrakce osobních údajů z daného modelu kýmkoli, kdo k němu přistupuje přímo, ale které mohou snížit pravděpodobnost extrakce osobních údajů souvisejících s trénovacími daty prostřednictvím dotazů.

3.2.2.2 Analýza modelu AI

54. Aby dozorové úřady mohly posoudit spolehlivost navrženého modelu AI, pokud jde o anonymizaci, je třeba nejprve zajistit, aby byl návrh vyvinut podle plánu a podléhal účinnému technickému řízení. Dozorové úřady by měly vyhodnotit, zda správci provedli veškeré audity založené na dokumentech (interní i externí), které zahrnují hodnocení zvolených opatření a jejich dopadu na omezení pravděpodobnosti identifikace. To by mohlo zahrnovat analýzu zpráv o přezkumech programu, jakož i teoretickou analýzu dokumentující vhodnost opatření zvolených ke snížení pravděpodobnosti opětovné identifikace dotčeného modelu.

3.2.2.3 Testování modelu AI a odolnost vůči útokům

55. V neposlední řadě by dozorové úřady měly zohlednit rozsah, četnost, množství a kvalitu testů, které správce na modelu provedl. Dozorové úřady by zejména měly vzít v úvahu, že úspěšné testování, které zahrnuje obecně známé útoky založené na nejmodernější technice, může být pouze důkazem odolnosti vůči těmto útokům. K datu vydání tohoto stanoviska to může zahrnovat mimo jiné strukturované testování proti: i) odvozování atributů a členství; ii) exfiltraci; iii) regurgitaci trénovacích dat; iv) invertování modelu nebo v) útokům za účelem rekonstrukce.

3.2.2.4 Dokumentace

56. Články 5, 24, 25 a 30 obecného nařízení o ochraně osobních údajů a v případech pravděpodobně vysokého rizika pro práva a svobody subjektů údajů článek 35 uvedeného nařízení vyžadují, aby správci odpovídajícím způsobem zdokumentovali své operace zpracování. To platí i pro jakékoli zpracování, které by zahrnovalo trénování modelu AI, a to i v případě, že cílem zpracování je anonymizace. Dozorové úřady by měly zvážit tuto dokumentaci a jakékoli pravidelné hodnocení následných rizik pro zpracování prováděné správci, neboť se jedná o základní kroky k doložení toho, že nejsou zpracovávány osobní údaje.
57. **EDPB se domnívá, že by dozorové úřady měly vzít v úvahu dokumentaci vždy, když je třeba vyhodnotit tvrzení o anonymitě týkající se daného modelu AI. EDPB konstatuje, že pokud dozorový úřad není po posouzení tvrzení o anonymitě, a to i s ohledem na dokumentaci, schopen potvrdit, že byla přijata účinná opatření k anonymizaci modelu AI, může se domnívat, že správce nesplnil své povinnosti týkající se odpovědnosti podle čl. 5 odst. 2 obecného nařízení o ochraně osobních údajů. Proto je třeba vzít v úvahu i soulad s jinými ustanoveními obecného nařízení o ochraně osobních údajů.**
58. Dozorové úřady by měly, pokud možno, ověřit, zda dokumentace správce obsahuje:

- a. veškeré informace týkající se posouzení vlivu na ochranu osobních údajů, včetně veškerých posouzení a rozhodnutí, v nichž byl vyvozen závěr, že posouzení vlivu na ochranu osobních údajů není nutné;
- b. veškeré rady nebo zpětnou vazbu poskytnutou pověřencem pro ochranu osobních údajů (pokud byl – nebo měl být – jmenován);
- c. informace o technických a organizačních opatřeních přijatých při navrhování modelu AI s cílem snížit pravděpodobnost identifikace, včetně modelu hrozeb a posouzení rizik, na nichž jsou tato opatření založena. To by mělo zahrnovat zvláštní opatření pro každý zdroj trénovacích souborů údajů, včetně příslušných zdrojových adres URL a popisů přijatých opatření (nebo opatření již přijatých poskytovateli souborů údajů, kteří jsou třetí stranou);
- d. technická a organizační opatření přijatá ve všech fázích životního cyklu modelu, která buď přispěla k nedostatku osobních údajů v modelu, nebo jej ověřila;
- e. dokumentaci dokládající teoretickou odolnost modelu AI vůči technikám opětovné identifikace, jakož i kontroly určené k omezení nebo posouzení úspěchu a dopadu hlavních útoků (regurgitace, útoků založených na odvozování členství, exfiltrace atd.). To může zahrnovat zejména: i) poměr mezi množstvím trénovacích dat a počtem parametrů v modelu, včetně analýzy jeho vlivu na model³⁸; ii) metriky pravděpodobnosti opětovné identifikace pomocí nejmodernější techniky; iii) zprávy o tom, jak byl model testován (kým, kdy, jak a v jakém rozsahu); a iv) výsledky testů;
- f. dokumentaci poskytnutou správcům používajícím model a/nebo subjektům údajů, zejména dokumentaci týkající se opatření přijatých ke snížení pravděpodobnosti identifikace a týkajících se možných zbytkových rizik.

3.3 Vhodnost oprávněného zájmu jako právního základu pro zpracování osobních údajů v souvislosti s vývojem a zaváděním modelů AI

59. V odpovědi na otázky č. 2 a 3 žádosti poskytne EDPB nejprve obecné připomínky k některým důležitým aspektům, které by měly dozorové úřady zohlednit bez ohledu na právní základ zpracování při posuzování toho, jak mohou správci doložit soulad s obecným nařízením o ochraně osobních údajů v souvislosti s modely AI. V návaznosti na pokyny 1/2024 ke zpracování osobních údajů na základě čl. 6 odst. 1 písm. f) obecného nařízení o ochraně osobních údajů³⁹ pak EDPB posoudí tři kroky, které jsou nutné k posouzení oprávněného zájmu v souvislosti s vývojem a zaváděním modelů AI.

³⁸ Ricciato F., *A Cautionary Reflection on (Pseudo-)Synthetic Data from Deep Learning on Personal Data* (Varovná úvaha o (pseudo)syntetických datech ze strojového učení, pokud jde o osobní údaje), konference Privacy in Statistical Databases (PSD 2024), Antibes, Francie, září 2024, snímky z prezentace k dispozici na adrese https://cros.ec.europa.eu/system/files/2024-10/20240926_PSD2024_Ricciato_v6_1.pdf a Belkin M., Hsu D., Ma S. a Mandal S. (2019), *Reconciling modern machine-learning practice and the classical bias–variance trade-off* (Nalezení souladu mezi moderními postupy strojového učení a klasickým kompromisem mezi zkreslením a odchylkou). Proceedings of the National Academy of Sciences, 24. července 2019, 116(32) 15849-15854, k dispozici na adrese <https://www.pnas.org/doi/10.1073/pnas.1903070116>.

³⁹ Viz pokyny EDPB 1/2024 ke zpracování osobních údajů na základě čl. 6 odst. 1 písm. f) obecného nařízení o ochraně osobních údajů, verze 1.0, přijaté dne 8. října 2024.

3.3.1 Obecné připomínky

60. EDPB připomíná, že obecné nařízení o ochraně osobních údajů nestanoví žádnou hierarchii mezi různými právními základy stanovenými v čl. 6 odst. 1 obecného nařízení o ochraně osobních údajů⁴⁰.
61. Článek 5 obecného nařízení o ochraně osobních údajů stanoví zásady zpracování osobních údajů. EDPB poukazuje na ty, které jsou pro toto stanovisko významné a které by měly dozorové úřady zohlednit přinejmenším při posuzování konkrétních modelů AI, jakož i nejdůležitějších požadavků z jiných ustanovení obecného nařízení o ochraně osobních údajů, a to s přihlédnutím k oblasti působnosti tohoto stanoviska.
62. **Zásada odpovědnosti** (čl. 5 odst. 2 obecného nařízení o ochraně osobních údajů) – Podle této zásady správce odpovídá za dodržování obecného nařízení o ochraně osobních údajů a musí být schopen toto dodržování doložit. V tomto ohledu by měly být úlohy a povinnosti stran, které zpracovávají osobní údaje v souvislosti s vývojem nebo zaváděním modelu AI, posouzeny před zahájením zpracování, aby byly od počátku vymezeny povinnosti správců nebo společných správců a (případně) zpracovatelů.
63. **Zásady zákonnosti, korektnosti a transparentnosti** (čl. 5 odst. 1 písm. a) obecného nařízení o ochraně osobních údajů) – Při posuzování zákonnosti zpracování v souvislosti s modely AI s ohledem na čl. 6 odst. 1 obecného nařízení o ochraně osobních údajů považuje EDPB za užitečné rozlišovat mezi jednotlivými fázemi zpracování osobních údajů⁴¹. Zásada korektnosti, která úzce souvisí se zásadou transparentnosti, vyžaduje, aby osobní údaje nebyly zpracovávány nespravedlivými metodami nebo na základě klamu nebo způsobem, který je „*pro subjekt údajů neoprávněně škodlivý, nezákonně diskriminační, neočekávaný nebo zavádějící*“⁴². Vzhledem ke složitosti využívaných technologií by proto měly být informace o zpracování osobních údajů v rámci modelů AI poskytovány přístupným, srozumitelným a uživatelsky přívětivým způsobem⁴³. Transparentnost zpracování osobních údajů zahrnuje zejména dodržování informačních povinností stanovených v člancích 12 až 14 obecného nařízení o ochraně osobních údajů⁴⁴, které v případě automatizovaného rozhodování, včetně profilování, rovněž vyžadují podávání smysluplných informací týkajících se použitého postupu, jakož i významu a předpokládaných důsledků takového zpracování pro subjekt údajů⁴⁵. Vzhledem k tomu, že fáze vývoje modelů AI mohou zahrnovat shromažďování velkého množství údajů z veřejně přístupných zdrojů (například prostřednictvím technik web scrapingu), je spoléhání se na výjimku stanovenou v čl. 14 odst. 5 písm. b) obecného nařízení o ochraně osobních údajů přísně omezeno na případy, kdy jsou v plném rozsahu splněny požadavky tohoto ustanovení⁴⁶.
64. **Zásady účelového omezení a minimalizace údajů** (čl. 5 odst. 1 písm. b) a c) obecného nařízení o ochraně osobních údajů) – V souladu se zásadou minimalizace údajů je pro vývoj a zavádění modelů AI nutné, aby osobní údaje byly přiměřené, relevantní a nezbytné ve vztahu k účelu. To může zahrnovat

⁴⁰ Tamtéž, odstavec 1.

⁴¹ Zpráva EDPB o práci vykonané pracovní skupinou ChatGPT, přijatá dne 23. května 2024, bod 14.

⁴² Zpráva EDPB o práci vykonané pracovní skupinou ChatGPT, přijatá dne 23. května 2024, bod 23; pokyny EDPB 4/2019 k článku 25 Záměrná a standardní ochrana osobních údajů, verze 2.0, přijaté dne 20. října 2020, bod 69; pokyny pracovní skupiny zřízené podle článku 29 k transparentnosti podle nařízení 2016/679 ve znění revidovaném a přijatém dne 11. dubna 2018, schválené EDPB dne 25. května 2018, bod 2.

⁴³ Pokyny pracovní skupiny zřízené podle článku 29 k transparentnosti podle nařízení 2016/679 ve znění revidovaném a přijatém dne 11. dubna 2018, schválené EDPB dne 25. května 2018, bod 5.

⁴⁴ Viz též 39. bod odůvodnění obecného nařízení o ochraně osobních údajů, v němž se uvádí, že „[p]ro fyzické osoby by mělo být transparentní, že osobní údaje, které se jich týkají, jsou shromažďovány, používány, konzultovány nebo jinak zpracovávány, jakož i v jakém rozsahu tyto osobní údaje jsou či budou zpracovávány [...]“.

⁴⁵ Čl. 13 odst. 2 písm. f) a čl. 14 odst. 2 písm. g) obecného nařízení o ochraně osobních údajů.

⁴⁶ Zpráva EDPB o práci vykonané pracovní skupinou ChatGPT, přijatá dne 23. května 2024, bod 27.

zpracování osobních údajů, aby se zabránilo rizikům možného zkreslení a chyb, pokud je to jasné a konkrétně určeno v rámci daného účelu a osobní údaje jsou pro tento účel nezbytné (např. účelu nelze účinně dosáhnout zpracováním jiných údajů, včetně syntetických nebo anonymizovaných údajů)⁴⁷. Pracovní skupina zřízená podle článku 29 již zdůraznila, že „*účel shromažďování musí být jasně a konkrétně určen* [...]“⁴⁸. Při posuzování, zda je sledovaný účel legitimní, určitý a výslovně vyjádřený a zda je zpracování v souladu se zásadou minimalizace údajů, je třeba nejprve určit, o jakou činnost zpracování se jedná. Je třeba připomenout, že jednotlivé dílčí fáze v rámci fáze vývoje nebo zavádění mohou představovat stejné nebo odlišné činnosti zpracování a mohou zahrnovat následné správce nebo společné správce. V některých případech je možné určit sledovaný účel během zavádění modelu AI v rané fázi vývoje. I v případě, že sledovaný účel určit nelze, by již měl být zřejmý určitý kontext zavedení modelu AI, a proto by mělo být zohledněno, jak tento kontext ovlivní účel vývoje. Při přezkumu účelu zpracování v dané fázi vývoje by dozorové úřady měly od správce (správců) očekávat určitou míru podrobností a vysvětlení, jak tyto podrobnosti ovlivňují účel zpracování. To může zahrnovat například informace o typu vyvinutého modelu AI, jeho očekávaných funkcích a jakémkoli jiném relevantním kontextu, který je v této fázi již znám. Kontext zavádění by mohl rovněž zahrnovat například to, zda je model vyvíjen pro interní použití, zda má správce v úmyslu model po jeho vývoji prodat nebo distribuovat třetím stranám, včetně toho, zda má být model primárně určen k použití pro výzkumné nebo komerční účely.

65. **Práva subjektů údajů** (kapitola III obecného nařízení o ochraně osobních údajů) – Bez ohledu na nutnost, aby dozorové úřady zajistily, aby při vypracovávání a zavádění modelů AI ze strany správců byla dodržována veškerá práva subjektů údajů, EDPB připomíná, že kdykoli správce používá jako právní základ oprávněný zájem, použije se a mělo by být zajištěno právo vznést námitku podle článku 21 obecného nařízení o ochraně osobních údajů⁴⁹.

3.3.2 Úvahy o třech krocích posuzování oprávněného zájmu v souvislosti s vývojem a zaváděním modelů AI

66. Aby bylo možné určit, zda dané zpracování osobních údajů může být založeno na čl. 6 odst. 1 písm. f) obecného nařízení o ochraně osobních údajů, měly by dozorové úřady ověřit, zda správci pečlivě posoudili a zdokumentovali, zda jsou splněny tyto tři kumulativní podmínky: i) sledování oprávněného zájmu správce nebo třetí strany; ii) nezbytnost zpracování osobních údajů pro uskutečnění sledovaného oprávněného zájmu a iii) před tímto zájmem nemají přednost zájmy nebo základní práva a svobody subjektu údajů⁵⁰.

⁴⁷ Kromě toho čl. 10 odst. 5 aktu o AI stanoví zvláštní pravidla pro zpracování zvláštních kategorií osobních údajů ve vztahu k vysoce rizikovým systémům AI za účelem zajištění detekce a oprav zkreslení.

⁴⁸ Stanovisko 3/2013 pracovní skupiny zřízené podle článku 29 k účelovému omezení (WP203), strany 15–16.

⁴⁹ Podle článku 21 obecného nařízení o ochraně osobních údajů platí, že pokud subjekt údajů z důvodů týkajících se jeho konkrétní situace vznesl námitku proti zpracování osobních údajů, které se jej týkají, správce osobní údaje dále nezpracovává, pokud neprokáže závažné oprávněné důvody pro zpracování, které převažují nad zájmy nebo právy a svobodami subjektu údajů, nebo pro určení, výkon nebo obhajobu právních nároků. Dozorové úřady proto musí vzít v úvahu oba aspekty, a to zda je správce schopen takové závažné převažující oprávněné důvody doložit a zda lze uplatnit právo vznést námitku.

⁵⁰ Rozsudek SDEU ze dne 4. července 2023, věc C-252/21, *Meta proti Bundeskartellamt* (ECLI:EU:C:2023:537), bod 106; rozsudek SDEU ze dne 11. prosince 2019, věc C-708/18, *Asociația de Proprietari bloc M5A-Scara A* (ECLI:EU:C:2019:1064), bod 40. Viz také pokyny EDPB 1/2024 ke zpracování osobních údajů na základě čl. 6 odst. 1 písm. f) obecného nařízení o ochraně osobních údajů, verze 1.0, přijaté dne 8. října 2024, bod 12 a násl.

3.3.2.1 První krok – Sledování oprávněného zájmu správce nebo třetí strany

67. Zájemem se rozumí širší zainteresovanost nebo prospěch, který může mít správce nebo třetí strana při provádění určité činnosti zpracování⁵¹. Ačkoli obecné nařízení o ochraně osobních údajů a SDEU uznaly několik zájmů jako oprávněných⁵², posouzení oprávněnosti daného konkrétního zájmu by mělo být výsledkem analýzy jednotlivých případů.
68. Jak připomíná EDPB ve svých pokynech k oprávněnému zájmu⁵³, zájem lze považovat za oprávněný, pokud jsou splněna tato tři kumulativní kritéria:
- a. zájem je v souladu s právními předpisy⁵⁴;
 - b. zájem je jasně a přesně vyjádřen a
 - c. zájem je skutečný a přítomný, nikoliv spekulativní.
69. S výhradou dalších dvou kroků vyžadovaných při posuzování oprávněného zájmu mohou v souvislosti s modely AI představovat oprávněný zájem tyto příklady: i) vývoj služby konverzačního agenta, který pomáhá uživatelům; ii) vývoj systému AI pro odhalování podvodného obsahu nebo chování a iii) zlepšení odhalování hrozeb v informačním systému.

3.3.2.2 Druhý krok – Analýza nezbytnosti zpracování pro uskutečnění sledovaného oprávněného zájmu

70. Druhý krok posouzení spočívá v určení, zda je zpracování osobních údajů nezbytné pro uskutečnění sledovaného oprávněného zájmu (oprávněných zájmů)⁵⁵ („test nezbytnosti“).
71. Ve 39. bodě odůvodnění obecného nařízení o ochraně osobních údajů se uvádí, že „[o]sobní údaje by měly být zpracovány pouze tehdy, nemůže-li být účelu zpracování přiměřeně dosaženo jinými prostředky“. Podle SDEU a předchozích pokynů EDPB by podmínka týkající se nezbytnosti zpracování měla být posuzována s ohledem na základní práva a svobody subjektů údajů a společně se zásadou

Jak je připomenuto v těchto pokynech, toto „posouzení by mělo být provedeno na začátku zpracování se zapojením pověřence pro ochranu osobních údajů (je-li jmenován) a mělo by být zdokumentováno správcem v souladu se zásadou odpovědnosti stanovenou v čl. 5 odst. 2 obecného nařízení o ochraně osobních údajů“.

⁵¹ Pokyny EDPB 1/2024 ke zpracování osobních údajů na základě čl. 6 odst. 1 písm. f) obecného nařízení o ochraně osobních údajů, verze 1.0, přijaté dne 8. října 2024, bod 14.

⁵² Pokyny EDPB 1/2024 ke zpracování osobních údajů na základě čl. 6 odst. 1 písm. f) obecného nařízení o ochraně osobních údajů, verze 1.0, přijaté dne 8. října 2024, bod 16.

⁵³ Pokyny EDPB 1/2024 ke zpracování osobních údajů na základě čl. 6 odst. 1 písm. f) obecného nařízení o ochraně osobních údajů, verze 1.0, přijaté dne 8. října 2024, bod 17.

⁵⁴ Rozsudek SDEU ze dne 4. října 2024, věc C-621/22, *Koninklijke Nederlandse Lawn Tennisbond* (ECLI:EU:C:2024:857), bod 49, kde SDEU zdůraznil, že oprávněný zájem nemůže být v rozporu se zákonem. V tomto ohledu EDPB zdůrazňuje, že při posuzování toho, zda je daný zájem v souladu s právními předpisy, je třeba případně zohlednit legislativní rámce. Viz například: čl. 26 odst. 3 a článek 28 nařízení Evropského parlamentu a Rady (EU) 2022/2065 ze dne 19. října 2022 o jednotném trhu digitálních služeb a o změně směrnice 2000/31/ES (nařízení o digitálních službách) týkající se zákazu reklamy cílené na nezletilé osoby; čl. 5 odst. 1 a 2 aktu o AI týkající se zakázaných postupů v oblasti AI (manipulativních praktik a podprahových technik mimo vědomí); zpracování v rozporu s právy duševního vlastnictví a ustanoveními směrnice (EU) 2019/790 o autorském právu a právech s ním souvisejících na jednotném digitálním trhu.

⁵⁵ Pokyny EDPB 1/2024 ke zpracování osobních údajů na základě čl. 6 odst. 1 písm. f) obecného nařízení o ochraně osobních údajů, verze 1.0, přijaté dne 8. října 2024, body 28–30.

„minimalizace údajů“ zakotvenou v čl. 5 odst. 1 písm. c) obecného nařízení o ochraně osobních údajů⁵⁶.

72. Metodika, na kterou se SDEU odvolává, zohledňuje kontext zpracování, jakož i dopady na správce a subjekty údajů. Posouzení nezbytnosti tedy zahrnuje dva prvky: i) zda činnost zpracování umožní dosažení sledovaného účelu⁵⁷ a ii) zda neexistuje méně rušivý způsob, jak tohoto účelu dosáhnout⁵⁸.
73. Například je třeba vzhledem k danému případu posoudit zamýšlený objem osobních údajů zahrnutých do modelu AI s ohledem na méně rušivé alternativy, které mohou být rozumně dostupné k dosažení stejně účinného účelu, jenž sleduje oprávněný zájem. Pokud je sledování účelu možné rovněž prostřednictvím takového modelu AI, který nevyžaduje zpracování osobních údajů, pak by zpracování osobních údajů nemělo být považováno za nezbytné. To je obzvláště důležité pro vývoj modelů AI. Při posuzování toho, zda je splněna podmínka nezbytnosti, by dozorové úřady měly věnovat zvláštní pozornost množství zpracovávaných osobních údajů a tomu, zda je přiměřené k prosazování daného oprávněného zájmu, a to i s ohledem na zásadu minimalizace údajů.
74. Při posuzování nezbytnosti by měl být rovněž zohledněn širší kontext zamýšleného zpracování osobních údajů. Existence prostředků, které jsou méně rušivé pro základní práva a svobody subjektů údajů, se může lišit v závislosti na tom, zda má správce přímý vztah se subjekty údajů (údaje první strany), či nikoli (údaje třetí strany). SDEU poskytl určité úvahy, které je třeba vzít v úvahu při analýze nezbytnosti zpracování osobních údajů první strany pro účely sledovaného oprávněného zájmu (oprávněných zájmů) (i když tak učinil v souvislosti se zpřístupněním těchto údajů třetím stranám)⁵⁹.

⁵⁶ Rozsudek SDEU ze dne 4. července 2023, věc C-252/21, *Meta proti Bundeskartellamt* (ECLI:EU:C:2023:537), body 108 a 109, rovněž s odkazem na rozsudek SDEU ze dne 11. prosince 2019, věc C-708/18, *Asociația de Proprietari bloc M5A-Scara A* (ECLI:EU:C:2019:1064), bod 48; rozsudek SDEU ze dne 9. listopadu 2010, spojené věci C-92/09 a C-93/09, *Volker und Markus Schecke* (ECLI:EU:C:2010:662), body 85 a 86; rozsudek SDEU ze dne 22. června 2021, věc C-439/19, *Latvijas Republikas Saeima* (ECLI:EU:C:2021:504), body 98, 109, 110, 113. Viz také například: pokyny EDPB 3/2019 ke zpracování osobních údajů prostřednictvím videotechniky, verze 2.0, přijaté dne 29. ledna 2020, body 24–26 a 73; pokyny EDPB 2/2019 o zpracovávání osobních údajů podle čl. 6 odst. 1 písm. b) GDPR v souvislosti s poskytováním on-line služeb subjektům údajů, verze 2.0, přijaté dne 8. října 2019, body 23–25; stanovisko EDPB č. 11/2024 k používání rozpoznávání obličeje pro zefektivnění toku cestujících na letištích, verze 1.1, přijaté dne 23. května 2024, bod 27.

⁵⁷ Viz rozsudek SDEU ze dne 16. prosince 2008, věc C-524/06, *Heinz Huber proti Spolkové republice Německo* (ECLI:EU:C:2008:724), bod 66. Rovněž ve stejné věci viz stanovisko generálního advokáta Poiaresse Madura ve věci C-524/06, *Heinz Huber proti Spolkové republice Německo* (ECLI:EU:C:2008:194), bod 16, v němž se uvádí: „zde je vhodným kritériem kritérium efektivity a přísluší vnitrostátním soudům, aby jej použily. Otázka, kterou musí klást, je, zda existují jiné způsoby zpracování údajů, při kterých mohou imigrační orgány uplatňovat pravidla statusu pobytu. Pokud takovou otázku zodpoví kladně, musí být centralizované uchovávání a zpracování údajů občanů Unie považováno za protiprávní. Není nutné, aby alternativní systém byl nejefektivnější nebo nejvhodnější; postačí bude-li schopen fungovat dostatečně. Jinými slovy, i když je centrální registr efektivnější, vhodnější nebo uživatelsky vstřícnější nežli jeho alternativy (jakými jsou decentralizované, místní registry), posledně uvedené systémy mají být jasně upřednostněny, pokud mohou být použity k uvedení statusu pobytu občanů [Unie].“

⁵⁸ Viz rozsudek SDEU ze dne 27. září 2017, věc C-73/16, *Peter Puškár* (ECLI:EU:C:2017:725), bod 113: „Předkládajícímu soudu tedy přísluší ověřit, zda vyhotovení sporného seznamu a zapsání jmen dotčených osob na uvedený seznam slouží k dosažení cílů, které jsou tím sledovány, a zda k dosažení uvedených cílů neexistují jiné, méně omezující prostředky“. Viz také například stanovisko generálního advokáta Rantose ve věci C-252/21, *Meta proti Bundeskartellamt*, ECLI:EU:C:2022:704, bod 61, v němž se uvádí: „[...] Proto je třeba, aby existovala úzká vazba mezi zpracováním a sledovaným zájmem, pokud neexistují alternativy, které by více respektovaly ochranu osobních údajů, protože nestačí, že zpracování závisí na prosté užitečnosti pro správce údajů.“

⁵⁹ Rozsudek SDEU ze dne 4. října 2024, věc C-621/22, *Koninklijke Nederlandse Lawn Tennisbond* (ECLI:EU:C:2024:857), body 51–53.

75. Ke splnění testu nezbytnosti může rovněž přispět zavedení technických záruk na ochranu osobních údajů. Mezi takové záruky může patřit například zavedení opatření, jako jsou opatření uvedená v oddíle 3.2.2, takovým způsobem, aby nedošlo k anonymizaci, ale aby se přesto ztížila identifikace subjektů údajů. EDPB konstatuje, že některá z těchto opatření, pokud nejsou vyžadována k dosažení souladu s obecným nařízením o ochraně osobních údajů, mohou představovat dodatečné záruky, jak je dále rozebráno v pododdíle „zmírňující opatření“ v rámci oddílu 3.3.2.3⁶⁰.

3.3.2.3 Třetí krok – Test vyváženosti

76. Třetím krokem posouzení oprávněného zájmu je „**vyvažování**“ (v tomto dokumentu se rovněž označuje pojmem „**test vyváženosti**“) ⁶¹. Tento krok spočívá v identifikaci a popisu různých protichůdných dotčených práv a zájmů⁶², tj. na jedné straně stojí zájmy, základní práva a svobody subjektů údajů a na druhé straně zájmy správce nebo třetí strany. Konkrétní okolnosti případu by pak měly být považovány za důkaz toho, že oprávněný zájem je vhodným právním základem pro dotčené činnosti zpracování⁶³.

Zájmy, základní práva a svobody subjektů údajů

77. V čl. 6 odst. 1 písm. f) obecného nařízení o ochraně osobních údajů se stanoví, že při posuzování jednotlivých složek v rámci testu vyváženosti by měl správce zohlednit zájmy, základní práva a svobody subjektů údajů. Zájmy subjektů údajů se rozumí ty, které mohou být ovlivněny dotčeným zpracováním. V souvislosti s fází vývoje modelu AI mohou k těmto zájmům patřit mimo jiné zájem na sebeurčení a zachování kontroly nad vlastními osobními údaji (např. údaji shromážděnými pro vývoj modelu). V souvislosti se zaváděním modelu AI mohou zájmy subjektů údajů zahrnovat mimo jiné zájmy na zachování kontroly nad vlastními osobními údaji (např. údaje zpracováváné po zavedení modelu), finanční zájmy (např. pokud je model AI používán subjektem údajů k vytváření příjmů nebo je používán fyzickou osobou v souvislosti s její profesní činností), osobní přínosy (např. pokud se model AI používá ke zlepšení dostupnosti určitých služeb) nebo socioekonomické zájmy (např. pokud model AI umožňuje přístup k lepší zdravotní péči nebo usnadňuje výkon základního práva, jako je přístup ke vzdělání)⁶⁴.
78. Čím přesněji je zájem definován s ohledem na zamýšlený účel zpracování, tím lépe umožní jasně pochopit reálné přínosy a rizika, které je třeba vzít při provádění testu vyváženosti v úvahu.
79. V souvislosti se základními právy a svobodami subjektů údajů může vývoj a zavádění modelů AI představovat vážná rizika pro práva chráněná Listinou základních práv EU (dále jen „**Listina EU**“), mimo jiné včetně práva na soukromý a rodinný život (článek 7 Listiny EU) a práva na ochranu osobních údajů (článek 8 Listiny EU). Tato rizika mohou nastat během fáze vývoje, například pokud jsou osobní údaje získány scrapingem v rozporu s přáními subjektů údajů nebo bez jejich vědomí. Tato rizika mohou nastat i ve fázi zavádění, například pokud jsou osobní údaje zpracovávány modelem (nebo jako součást modelu) způsobem, který je v rozporu s právy subjektů údajů, nebo pokud je možné odvodit, a to náhodně nebo prostřednictvím útoku (např. odvození členství, extrakce nebo invertování modelu),

⁶⁰ Viz pokyny EDPB 1/2024 ke zpracování osobních údajů na základě čl. 6 odst. 1 písm. f) obecného nařízení o ochraně osobních údajů, verze 1.0, přijaté dne 8. října 2024, bod 57.

⁶¹ Viz pokyny EDPB 1/2024 ke zpracování osobních údajů na základě čl. 6 odst. 1 písm. f) obecného nařízení o ochraně osobních údajů, verze 1.0, přijaté dne 8. října 2024, bod 31 až 60.

⁶² Viz pokyny EDPB 1/2024 ke zpracování osobních údajů na základě čl. 6 odst. 1 písm. f) obecného nařízení o ochraně osobních údajů, verze 1.0, přijaté dne 8. října 2024, bod 32.

⁶³ Viz pokyny EDPB 1/2024 ke zpracování osobních údajů na základě čl. 6 odst. 1 písm. f) obecného nařízení o ochraně osobních údajů, verze 1.0, přijaté dne 8. října 2024, bod 32, rovněž odkazující na rozsudek SDEU ze dne 4. července 2023, věc C-252/21, *Meta proti Bundeskartellamt* (ECLI:EU:C:2023:537), bod 110.

⁶⁴ Viz pokyny EDPB 1/2024 ke zpracování osobních údajů na základě čl. 6 odst. 1 písm. f) obecného nařízení o ochraně osobních údajů, verze 1.0, přijaté dne 8. října 2024, bod 38.

jaké osobní údaje jsou obsaženy v databázi použité pro učení. Takové situace představují riziko pro soukromí subjektů údajů, jejichž údaje by se mohly objevit ve fázi zavádění systému AI (např. riziko poškození dobré pověsti, krádež nebo zneužití identity, bezpečnostní riziko v závislosti na povaze údajů).

80. V závislosti na konkrétním případě mohou být ohrožena i jiná základní práva. Například rozsáhlé a nerozlišující shromažďování údajů modely AI ve fázi vývoje může u subjektů údajů vytvořit pocit, že jsou sledovány, zejména s ohledem na obtíže spojené se zabráněním tomu, aby byly veřejné údaje získávány scrapingem. To může vést jednotlivce k autocenzuře a představovat riziko narušení jejich svobody projevu (článek 11 Listiny EU). I ve fázi zavádění jsou přítomna rizika pro svobodu projevu, pokud se modely AI používají k blokování zveřejňování obsahu od subjektů údajů. Kromě toho může model AI doporučující nevhodný obsah zranitelným osobám představovat riziko pro jejich duševní zdraví (čl. 3 odst. 1 Listiny EU). V jiných případech může mít zavedení modelů AI také nepříznivé důsledky pro právo jednotlivce na práci (článek 15 Listiny EU), například když jsou žádosti o zaměstnání předvybrány pomocí modelu AI. Stejně tak by model AI mohl představovat rizika pro právo na zákaz diskriminace (článek 21 Listiny EU), pokud diskriminuje jednotlivce na základě určitých osobních charakteristik (jako je státní příslušnost nebo pohlaví). Kromě toho může zavedení modelů AI představovat také rizika pro bezpečnost jednotlivce (např. v případě, že je model AI používán se zlým úmyslem), jakož i rizika pro jeho fyzickou a duševní nedotknutelnost⁶⁵.
81. Zavedení modelů AI může mít rovněž pozitivní dopad na některá základní práva, např. model může podpořit právo na duševní nedotknutelnost osoby (článek 3 Listiny), například když se model AI používá k identifikaci škodlivého obsahu na internetu, nebo model může usnadnit přístup k některým základním službám nebo usnadnit výkon základních práv, jako je přístup k informacím (článek 11 Listiny EU) nebo přístup ke vzdělání (článek 14 Listiny EU).

Dopad zpracování na subjekty údajů

82. Zpracování osobních údajů, k němuž dochází ve fázích vývoje a zavádění modelů AI, může mít na subjekty údajů různý dopad, který může být pozitivní nebo negativní⁶⁶. Pokud například činnost zpracování přináší subjektu údajů výhody, lze je v testu vyváženosti zohlednit. Ačkoli existence těchto výhod může ze strany dozorového úřadu vést k závěru, že zájmy, základní práva a svobody subjektů údajů nepřevažují nad zájmy správce nebo třetí strany, k takovému závěru lze dospět pouze na základě výsledku analýzy jednotlivých případů zohledňující všechny příslušné faktory.
83. Dopad zpracování na subjekty údajů může být ovlivněn i) povahou údajů zpracovávaných modely; ii) kontextem zpracování a iii) dalšími důsledky, které může zpracování mít⁶⁷.
84. Pokud jde o **povahu zpracovávaných údajů**, je třeba připomenout, že kromě zvláštních kategorií osobních údajů a údajů týkajících se rozsudků v trestních věcech a trestných činů, které požívají dodatečné ochrany podle článků 9 a 10 obecného nařízení o ochraně osobních údajů, může k významným důsledkům pro subjekty údajů vést zpracování i některých jiných kategorií osobních údajů. V této souvislosti by se za zpracování, které může mít závažný dopad na subjekty údajů, mělo pro účely vývoje a zavedení modelu AI považovat zpracování určitých druhů osobních údajů, které odhalují vysoce soukromé informace (např. finanční údaje nebo údaje o poloze). Ve fázi zavádění

⁶⁵ Pokyny EDPB 1/2024 ke zpracování osobních údajů na základě čl. 6 odst. 1 písm. f) obecného nařízení o ochraně osobních údajů, verze 1.0, přijaté dne 8. října 2024, bod 46.

⁶⁶ Viz pokyny EDPB 1/2024 ke zpracování osobních údajů na základě čl. 6 odst. 1 písm. f) obecného nařízení o ochraně osobních údajů, verze 1.0, přijaté dne 8. října 2024, bod 39.

⁶⁷ Viz pokyny EDPB 1/2024 ke zpracování osobních údajů na základě čl. 6 odst. 1 písm. f) obecného nařízení o ochraně osobních údajů, verze 1.0, přijaté dne 8. října 2024, bod 32.

mohou být důsledky takového zpracování pro subjekty údajů například ekonomické (např. diskriminace v souvislosti se zaměstnáním) a/nebo reputační (např. pomluva).

85. V souvislosti s **kontextem zpracování** je nejprve nutné určit prvky, které by mohly pro subjekty údajů představovat riziko (např. způsob, jakým byl model vyvinut, způsob, jakým může být model zaveden, a/nebo zda jsou bezpečnostní opatření použita k ochraně osobních údajů vhodná). Při určování těchto potenciálních příčin hrají klíčovou úlohu povaha modelu a zamýšlené provozní použití.
86. Je rovněž nutné posoudit závažnost těchto rizik pro subjekty údajů. Lze mimo jiné zvážit, jak jsou osobní údaje zpracovávány (např. jsou-li kombinovány s jinými soubory údajů), jaký je rozsah zpracování a množství zpracovávaných osobních údajů⁶⁸ (např. celkový objem údajů, objem údajů připadajících na jeden subjekt údajů, počet dotčených subjektů údajů)⁶⁹, status subjektu údajů (např. děti nebo jiné zranitelné subjekty údajů) a jejich vztah se správcem (např. je-li subjekt údajů zákazníkem). Například používání web scrapingu ve fázi vývoje může mít, pokud neexistují dostatečné záruky, významný dopad na jednotlivce, a to z důvodu velkého objemu shromažďovaných údajů, velkého počtu subjektů údajů a nerozlišujícího shromažďování osobních údajů.
87. Při posuzování dopadu zpracování na subjekty údajů je třeba vzít v úvahu také **další důsledky**, které může zpracování mít. Dozorové úřady by je měly posuzovat případ od případu s ohledem na konkrétní předmětné skutečnosti.
88. Mezi tyto důsledky mohou patřit (mimo jiné) rizika porušení základních práv subjektů údajů, jak je popsáno v předchozím pododdíle⁷⁰. Rizika se mohou lišit co do pravděpodobnosti a závažnosti a mohou vyplývat ze zpracování osobních údajů, které by mohlo vést k fyzické, hmotné nebo nehmotné újmě, zejména pokud by zpracování mohlo vyústit v diskriminaci⁷¹.
89. Pokud zavedení modelu AI zahrnuje zpracování osobních údajů jak i) subjektů údajů, jejichž osobní údaje jsou zahrnuty v souboru údajů použitém ve fázi vývoje; tak ii) subjektů údajů, jejichž osobní údaje jsou zpracovávány ve fázi zavedení, měly by dozorové úřady při ověřování testu vyváženosti prováděného správcem rozlišovat a zvažovat rizika ovlivňující zájmy, práva a svobody každé z těchto kategorií subjektů údajů.
90. **V neposlední řadě by se při analýze možných dalších důsledků zpracování měla zohlednit také pravděpodobnost, že se tyto další důsledky projeví.** Posouzení této pravděpodobnosti by mělo být provedeno s ohledem na zavedená technická a organizační opatření a zvláštní okolnosti případu. Dozorové úřady mohou například zvážit, zda byla zavedena opatření k zamezení možného zneužití modelu AI. V případě modelů AI, které mohou být zavedeny k různým účelům, jako je generativní AI, to může zahrnovat kontroly, které co nejvíce omezí jejich používání ke škodlivým praktikám, například: vytváření deep fakes; chatboty, které jsou používány k šíření dezinformací, k phishingu a jiným druhům podvodů, a manipulativní AI / agenti AI (zejména pokud jsou antropomorfní nebo poskytují zavádějící informace).

⁶⁸ Viz pokyny EDPB 1/2024 ke zpracování osobních údajů na základě čl. 6 odst. 1 písm. f) obecného nařízení o ochraně osobních údajů, verze 1.0, přijaté dne 8. října 2024, bod 43.

⁶⁹ Rozsudek SDEU ze dne 4. července 2023, věc C-252/21, *Meta proti Bundeskartellamt* (ECLI:EU:C:2023:537), bod 116.

⁷⁰ Viz pododdíl „Zájmy, základní práva a svobody subjektů údajů“ výše.

⁷¹ Viz oddíl 2.3 pokynů EDPB 1/2024 ke zpracování osobních údajů na základě čl. 6 odst. 1 písm. f) obecného nařízení o ochraně osobních údajů, verze 1.0, přijaté dne 8. října 2024. Další příklady naleznete také v 75. bodě odůvodnění obecného nařízení o ochraně osobních údajů.

Přiměřená očekávání subjektů údajů

91. Na základě 47. bodu odůvodnění obecného nařízení o ochraně osobních údajů je „*existenci oprávněného zájmu v každém případě třeba pečlivě posoudit, včetně toho, zda subjekt údajů může v okamžiku a v kontextu shromažďování osobních údajů důvodně očekávat, že ke zpracování pro tento účel může dojít. Zájmy a základní práva subjektu údajů by mohly převážet nad zájmy správce údajů zejména tehdy, jestliže ke zpracování osobních údajů dochází za okolností, kdy subjekt údajů jejich další zpracování důvodně neočekává.*“⁷²
92. Přiměřená očekávání hrají v testu vyváženosti klíčovou úlohu, v neposlední řadě kvůli složitosti technologie používané v modelech AI a skutečnosti, že pro subjekty údajů může být obtížné pochopit rozmanitost potenciálních použití modelu AI a související zpracování osobních údajů⁷³. Za tímto účelem lze zvážit informace poskytované subjektům údajů při posuzování toho, zda mohou subjekty údajů důvodně očekávat, že budou jejich osobní údaje zpracovány. I když neposkytnutí informací může přispět k tomu, aby subjekty údajů neočekávaly určité zpracování, pouhé splnění požadavků na transparentnost stanovených v obecném nařízení o ochraně osobních údajů však není samo o sobě dostačující k tomu, aby bylo možné mít za to, že subjekty údajů mohou přiměřeně očekávat určité zpracování⁷⁴. Navíc pouhá skutečnost, že informace týkající se fáze vývoje modelu AI jsou zahrnuty do zásad ochrany osobních údajů vypracovaných správcem, nemusí nutně znamenat, že subjekty údajů mohou přiměřeně očekávat, že ke zpracování dojde. Tuto skutečnost by naopak měly dozorové úřady analyzovat s ohledem na konkrétní okolnosti případu a všechny relevantní faktory.
93. Při posuzování přiměřených očekávání subjektů údajů v souvislosti se zpracováním, k němuž dochází ve fázi vývoje, je důležité odkázat na prvky uvedené v pokynech EDPB k oprávněnému zájmu⁷⁵. Dále je v rámci tématu tohoto stanoviska důležité zohlednit širší kontext zpracování. Ten může zahrnovat, avšak nikoliv výlučně, to, zda osobní údaje byly veřejně dostupné, či nikoli, povahu vztahu mezi subjektem údajů a správcem (a zda mezi nimi existuje vazba), povahu služby, kontext, v němž byly osobní údaje shromážděny, zdroj, z něhož byly údaje shromážděny (např. internetové stránky nebo služba, odkud byly osobní údaje shromážděny, a nastavení ochrany osobních údajů, které nabízejí), potenciální další využití modelu a to, zda si subjekty údajů jsou skutečně vědomy toho, že jejich osobní údaje jsou na internetu.
94. Ve fázi vývoje modelu se mohou přiměřená očekávání subjektů údajů lišit v závislosti na tom, zda údaje zpracovávají pro vývoj modelu subjekty údajů zveřejnily, či nikoli. Dále se mohou přiměřená očekávání lišit také v závislosti na tom, zda údaje poskytly správci přímo (např. v souvislosti s využíváním služby), nebo zda je správce získal z jiného zdroje (např. prostřednictvím třetí strany nebo

⁷² Viz také rozsudek SDEU ze dne 4. července 2023, věc C-252/21, *Meta proti Bundeskartellamt* (ECLI:EU:C:2023:537), bod 112; rozsudek SDEU ze dne 11. prosince 2019, věc C-708/18, *Asociația de Proprietari bloc M5A-Scara A* (ECLI:EU:C:2019:1064), bod 58; rozsudek SDEU ze dne 4. října 2024, C-621/22, *Koninklijke Nederlandse Lawn Tennisbond* (ECLI:EU:C:2024:857), bod 55.

⁷³ Například v rozsudku ze dne 4. července 2023, věc C-252/21, *Meta proti Bundeskartellamt* (ECLI:EU:C:2023:537), bod 123, SDEU sice konstatoval, že „zlepšení produktu“ nelze v zásadě vyloučit jako oprávněný zájem, ale zároveň konstatoval, že „*lze pochybovat o tom, že [...] může mít cíl spočívající ve zlepšení produktu s ohledem na rozsah tohoto zpracování a jeho významný dopad na uživatele, jakož i okolnost, že uživatel nemůže rozumně očekávat, že tyto údaje budou zpracovány [...], přednost před zájmy a základními právy takového uživatele, a to tím spíše v případě, že se jedná o dítě*“.

⁷⁴ Pokyny EDPB 1/2024 ke zpracování osobních údajů na základě čl. 6 odst. 1 písm. f) obecného nařízení o ochraně osobních údajů, verze 1.0, přijaté dne 8. října 2024, bod 53.

⁷⁵ Pokyny EDPB 1/2024 ke zpracování osobních údajů na základě čl. 6 odst. 1 písm. f) obecného nařízení o ochraně osobních údajů, verze 1.0, přijaté dne 8. října 2024, body 50–54.

scrapingu). V obou případech je třeba při posuzování přiměřených očekávání zohlednit kroky, které byly podniknuty za účelem informování subjektů údajů o činnostech zpracování.

95. Ve fázi zavádění modelu AI je stejně důležité zohlednit přiměřená očekávání subjektů údajů v souvislosti s konkrétními schopnostmi modelu. Například u modelů AI, které se mohou přizpůsobovat v závislosti na poskytnutých vstupech, může být relevantní zvážit, zda si subjekty údajů byly vědomy, že poskytly osobní údaje, aby model AI mohl přizpůsobit své reakce jejich potřebám a aby mohly získat služby na míru. Kromě toho může být rovněž důležité zvážit, zda by tato činnost zpracování ovlivnila pouze službu poskytovanou dotčeným subjektům údajů (např. personalizaci obsahu pro konkrétního uživatele), nebo zda by byla použita k úpravě služby poskytované všem zákazníkům (např. za účelem obecného zlepšení modelu). Stejně jako ve fázi vývoje může být obzvláště důležité zvážit, zda existuje přímá vazba mezi subjekty údajů a správcem. Taková přímá vazba může například správci umožnit snadné poskytování informací o činnosti zpracování a modelu subjektům údajů, což by mohlo mít následně vliv na přiměřená očekávání těchto subjektů údajů.

Zmírňující opatření

96. Pokud se zdá, že zájmy, práva a svobody subjektů údajů převažují nad oprávněným zájmem (oprávněnými zájmy) správce nebo třetí strany, může správce zvážit zavedení zmírňujících opatření, aby omezil dopad zpracování na tyto subjekty údajů. Zmírňující opatření jsou záruky, které by měly být přizpůsobeny okolnostem daného případu, a závisí na různých faktorech, včetně zamýšleného použití modelu AI. Cílem těchto zmírňujících opatření má být zajistit, aby zájmy správce nebo třetí strany nepřevažovaly, a správce by tudíž mohl vycházet z tohoto právního základu.
97. Jak se připomíná v pokynech EDPB k oprávněnému zájmu, zmírňující opatření by neměla být zaměňována s opatřeními, která je správce podle právních předpisů povinen v každém případě přijmout k zajištění souladu s obecným nařízením o ochraně osobních údajů, a to bez ohledu na to, zda je zpracování založeno na čl. 6 odst. 1 písm. f) obecného nařízení o ochraně osobních údajů, či nikoliv⁷⁶. To je obzvláště důležité u opatření, která například vyžadují dodržování zásad obecného nařízení o ochraně osobních údajů, jako je zásada minimalizace údajů.
98. Níže uvedený výčet opatření je demonstrativní a nepreskriptivní a je třeba zvážit provádění opatření na základě posouzení v daném jednotlivém případě. Ačkoli v závislosti na okolnostech může být nutné, aby některá z níže uvedených opatření byla uvedena do souladu s konkrétními povinnostmi podle obecného nařízení o ochraně osobních údajů, v opačném případě mohou být vzata v úvahu jako dodatečné záruky. Kromě toho se některá z níže uvedených opatření týkají oblastí, v nichž dochází k rychlému vývoji a změnám, a to by měly dozorové úřady zohlednit při projednávání konkrétního případu.
99. **V souvislosti s fází vývoje modelů AI** lze přijmout několik opatření ke zmírnění rizik, která představuje zpracování osobních údajů první i třetí strany (včetně zmírnění rizik souvisejících s praktikami web scrapingu). Na základě výše uvedených skutečností EDPB uvádí některé příklady opatření, která mohou být zavedena ke zmírnění rizik zjištěných při testu vyváženosti a která by dozorové úřady měly v jednotlivých případech zohlednit při posuzování konkrétních modelů AI.
100. **Technická opatření:**
- a. Opatření uvedená v oddíle 3.2.2, která jsou vhodná ke zmírnění příslušných rizik, pokud tato opatření nevedou k anonymizaci modelu a nejsou vyžadována ke splnění jiných povinností

⁷⁶ Pokyny EDPB 1/2024 ke zpracování osobních údajů na základě čl. 6 odst. 1 písm. f) obecného nařízení o ochraně osobních údajů, verze 1.0, přijaté dne 8. října 2024, bod 57.

podle obecného nařízení o ochraně osobních údajů nebo v rámci testu nezbytnosti (druhý krok posouzení oprávněného zájmu).

101. Kromě těchto opatření mohou další relevantní opatření zahrnovat:

- b. Pseudonymizační opatření: ta by například mohla zahrnovat opatření k zamezení jakékoliv kombinace údajů založených na individuálních identifikátorech. Tato opatření nemusí být vhodná, pokud se dozorový úřad domnívá, že správce prokázal přiměřenou nutnost shromáždit různé údaje o konkrétní fyzické osobě pro účely vývoje daného systému nebo modelu AI.
- c. Opatření k maskování osobních údajů nebo jejich nahrazení v trénovacím souboru falešnými osobními údaji (např. nahrazení jmen a e-mailových adres falešnými jmény a falešnými e-mailovými adresami). Toto opatření může být obzvláště vhodné v případě, že skutečný věcný obsah údajů není relevantní pro celkové zpracování (např. při trénování velkých jazykových modelů).

102. **Opatření, která usnadňují výkon práv jednotlivců:**

- a. Dodržování přiměřené doby mezi shromážděním trénovacího souboru údajů a jeho použitím. Tato dodatečná záruka může subjektům údajů umožnit výkon jejich práva během uvedeného období, přičemž přiměřená doba se posuzuje v závislosti na okolnostech každého případu.
- b. Návrh bezpodmínečné „možnosti nezúčastnit se“ od samého počátku, například poskytnutí diskrečního práva vznést námitku subjektům údajů předtím, než dojde ke zpracování, s cílem posílit kontrolu fyzických osob nad jejich údaji, což překračuje podmínky stanovené v článku 21 obecného nařízení o ochraně osobních údajů⁷⁷.
- c. Umožnění subjektům údajů vykonávat jejich právo na výmaz i v případě, že se nepoužijí zvláštní důvody uvedené v čl. 17 odst. 1 obecného nařízení o ochraně osobních údajů⁷⁸.
- d. Stanovení, aby subjekty údajů mohly předkládat požadavky týkající se regurgitace nebo zapamatování údajů, a určení okolností a prostředků, jimiž mohou být nároky reprodukovány, a umožnění správcům reprodukovat a posuzovat příslušné techniky „odučení“ za účelem zjednání nápravy, pokud jde o tyto požadavky.

103. **Opatření v oblasti transparentnosti:** v některých případech by mezi zmírňující opatření mohla patřit opatření, která zajišťují větší transparentnost, pokud jde o vývoj modelu AI. Některá opatření mohou kromě dodržování povinností podle obecného nařízení o ochraně osobních údajů pomoci překonat informační asymetrii a umožnit subjektům údajů lépe porozumět zpracování, které je součástí fáze vývoje:

- a. Zpřístupnění veřejné a snadno přístupné komunikace, která přesahuje rámec informací požadovaných podle článků 13 nebo 14 obecného nařízení o ochraně osobních údajů, například poskytnutím dalších podrobností o kritériích shromažďování a všech použitých souborech údajů, a to s přihlédnutím ke zvláštní ochraně dětí a zranitelných osob.
- b. Alternativní formy informování subjektů údajů, například: mediální kampaně v různých sdělovacích prostředcích s cílem informovat subjekty údajů, informační kampaň prostřednictvím e-mailu, využití grafické vizualizace, často kladené otázky, označení

⁷⁷ Tamtéž.

⁷⁸ Tamtéž.

transparentnosti a modelové karty, jejichž systematizace by mohla vytvořit strukturu pro prezentaci informací o modelech AI, a dobrovolné výroční zprávy o transparentnosti.

104. **Zvláštní zmírňující opatření v souvislosti s web scrapingem:** Vzhledem k tomu, že, jak bylo uvedeno výše, web scraping přináší specifická rizika⁷⁹, lze v této souvislosti určit zvláštní zmírňující opatření. Ve vhodných případech je mohou dozorové úřady kromě výše uvedených zmírňujících opatření zvážit při vyšetřování správců provádějících web scraping.
105. Zvláštní opatření, pokud nejsou nezbytná v rámci druhého kroku posouzení oprávněného zájmu, se mohou ukázat jako užitečná pro zmírnění rizika v souvislosti s web scrapingem. Mohou zahrnovat **technická opatření**, jako jsou:
- a. vyloučení obsahu údajů z publikací, které by mohly obsahovat osobní údaje představující riziko pro určité osoby nebo skupiny osob (např. osoby, které by mohly být v případě zveřejnění informací vystaveny zneužití, předsudkům, nebo dokonce fyzické újmě);
 - b. zajištění toho, aby nebyly shromažďovány určité kategorie údajů nebo aby byly ze shromažďování údajů vyloučeny určité zdroje. To by mohlo zahrnovat například určité internetové stránky, které obzvláště zasahují do soukromí z důvodu citlivosti daného tématu;
 - c. vyloučení shromažďování z určitých internetových stránek (nebo částí internetových stránek), které jednoznačně vznášejí námitky proti používání web scrapingu a opakovaného použití jejich obsahu pro účely vytváření trénovacích databází pro AI (například respektováním souborů robots.txt nebo ai.txt nebo jakéhokoli jiného uznávaného mechanismu pro vyjádření vyloučení z automatického procházení internetových stránek nebo scrapingu);
 - d. stanovení jiných relevantních omezení pro shromažďování, případně včetně kritérií založených na časových lhůtách.
106. V souvislosti s web scrapingem mohou příklady konkrétních opatření **usnadňujících výkon práv fyzických osob a transparentnost** zahrnovat: vytvoření seznamu subjektů, které si výslovně nepřejí zpracování svých údajů, jenž spravuje správce a který subjektům údajů umožňuje vznést námitku proti shromažďování jejich údajů na určitých internetových stránkách nebo on-line platformách tím, že poskytnou informace, které je na těchto internetových stránkách identifikují, a to i předtím, než dojde ke shromažďování údajů⁸⁰.
107. **Zvláštní aspekty týkající se zmírňujících opatření ve fázi zavádění:** Ačkoli některá z výše uvedených opatření mohou být v závislosti na okolnostech relevantní i pro fázi zavádění, EDPB níže uvádí demonstrativní výčet dalších podpůrných opatření, která mohou být provedena a která by dozorové úřady měly posuzovat případ od případu.
- a. Mohou být například zavedena **technická opatření**, aby se zabránilo ukládání, regurgitaci nebo vytváření osobních údajů, zejména v souvislosti s generativními modely AI (jako jsou výstupní filtry), a/nebo aby se zmírnilo riziko nezákonného opětovného použití modely AI pro obecné účely (např. digitální vodoznaky výstupů vytvořených umělou inteligencí).

⁷⁹ Tyto praktiky mohou rovněž vyvolat další problémy, kterými se toto stanovisko nezabývá, viz například Pagallo U., Ciani Sciolla J., *Anatomy of web data scraping: ethics, standards, and the problems of the law* (Anatomie extrakce dat z internetu pomocí web scrapingu: etika, normy a problémy spojené s právními předpisy). European Journal of Privacy Law & Technologies, (2023) 2, s. 1–19, k dispozici na adrese <https://doi.org/10.57230/EJPLT232PS>.

⁸⁰ Pokud správce neprokáže závažné oprávněné důvody pro zpracování, které převažují nad zájmy nebo právy a svobodami subjektu údajů, nebo pro určení, výkon nebo obhajobu právních nároků.

- b. **Opatření, která usnadňují nebo urychlují výkon práv fyzických osob** ve fázi zavádění nad rámec toho, co vyžadují právní předpisy, zejména – nikoli však výlučně – pokud jde o výkon práva na výmaz osobních údajů z výstupních dat modelu nebo deduplikaci údajů a metody po vytrénování modelu, které se snaží odstranit nebo potlačit osobní údaje.

108. Při zkoumání zavedení konkrétního modelu AI by měly dozorové úřady zvážit, zda správce zveřejnil provedený test vyváženosti, protože to může zvýšit transparentnost a korektnost. Jak je uvedeno v pokynech EDPB k oprávněnému zájmu, lze zvážit i další opatření, která subjektům údajů poskytnou informace získané z testu vyváženosti před jakýmkoli shromažďováním osobních údajů⁸¹. EDPB rovněž opakuje⁸², že jedním z prvků, které je třeba vzít v úvahu, je to, zda správce případně zapojil pověřence pro ochranu osobních údajů.

3.4 Možný dopad protiprávního zpracování při vývoji modelu AI na zákonnost následného zpracování nebo provozu modelu AI

109. Tato část stanoviska se zabývá otázkou č. 4 žádosti. Účelem této otázky je vyjasnit možný dopad protiprávního zpracování ve fázi vývoje na následné zpracování (například ve fázi zavádění modelu AI) nebo na provoz modelu. Otázka se snaží postihnout jak situaci, kdy takový model AI zpracovává osobní údaje, které jsou uchovávány v modelu (otázka č. 4 bod i) žádosti), tak situaci, kdy při zavedení modelu AI již nedochází ke zpracování osobních údajů (tj. model je anonymní) (otázka č. 4 bod ii) žádosti).
110. Předtím, než se EDPB začne zabývat některými konkrétními scénáři, uvádí následující obecné úvahy.
111. Zprvce vysvětlení uvedená v tomto oddíle se zaměří na zpracování osobních údajů ve fázi vývoje, při kterém došlo k porušení zásady zákonnosti stanovené konkrétně v čl. 5 odst. 1 písm. a) a článku 6 obecného nařízení o ochraně osobních údajů (dále jen „**protiprávnost**“)⁸³. Ve stejném duchu se tedy úvahy EDPB zaměří na dopad protiprávnosti zpracování ve fázi vývoje na zákonnost následného zpracování nebo provozu modelu (tj. na soulad s čl. 5 odst. 1 písm. a) a článkem 6 obecného nařízení o ochraně osobních údajů). EDPB však poukazuje na to, že zpracování prováděné ve fázi vývoje může rovněž vést k porušení jiných ustanovení obecného nařízení o ochraně osobních údajů, jako je nedostatečná transparentnost vůči subjektům údajů nebo záměrná a/nebo standardní ochrana osobních údajů, které nejsou v tomto stanovisku rozebírány.
112. Zadruhé při zodpovídání této otázky hraje klíčovou úlohu zásada odpovědnosti, která vyžaduje, aby správci byli odpovědní za dodržování *mimo jiné* čl. 5 odst. 1 a článku 6 obecného nařízení o ochraně osobních údajů⁸⁴ a doložili soulad s nimi. To platí i pro nutnost posoudit, která organizace je správcem dotčené činnosti zpracování a zda nastanou situace společných správců (neboť spolu mohou být nerozlučně spojené)⁸⁵. Vzhledem k významu skutkových okolností každého případu, a to i s ohledem na úlohu, kterou hrají jednotlivé strany zapojené do zpracování, by úvahy EDPB měly být chápány jako obecné připomínky, které by měly dozorové úřady posuzovat případ od případu.

⁸¹ Pokyny EDPB 1/2024 ke zpracování osobních údajů na základě čl. 6 odst. 1 písm. f) obecného nařízení o ochraně osobních údajů, verze 1.0, přijaté dne 8. října 2024, bod 68.

⁸² Pokyny EDPB 1/2024 ke zpracování osobních údajů na základě čl. 6 odst. 1 písm. f) obecného nařízení o ochraně osobních údajů, verze 1.0, přijaté dne 8. října 2024, bod 12.

⁸³ Rozsudek SDEU ze dne 4. května 2023, věc C-60/22, *Bundesrepublik Deutschland* (ECLI:EU:C:2023:373), body 55–57.

⁸⁴ Rozsudek SDEU ze dne 4. května 2023, věc C-60/22, *Bundesrepublik Deutschland* (ECLI:EU:C:2023:373), bod 53.

⁸⁵ Pokyny EDPB 07/2020 k pojmům správce a zpracovatele v GDPR, verze 2.1, přijato dne 7. července 2021, bod 55.

113. Zatřetí EDPB zdůrazňuje, že v souladu s čl. 51 odst. 1 obecného nařízení o ochraně osobních údajů jsou dozorové úřady „pověřeny monitorováním uplatňování [obecného nařízení o ochraně osobních údajů] s cílem chránit základní práva a svobody fyzických osob v souvislosti se zpracováním jejich osobních údajů a usnadnit volný pohyb osobních údajů uvnitř Unie“. Je proto v pravomoci dozorových úřadů posuzovat zákonnost zpracování a vykonávat jejich pravomoci udělené obecným nařízením o ochraně osobních údajů v souladu s jejich vnitrostátním rámcem⁸⁶. V takových případech mají vnitrostátní dozorové úřady diskreční pravomoc posoudit možné (možná) porušení a zvolit vhodná, nezbytná a přiměřená opatření z těch, která jsou uvedena v článku 58 obecného nařízení o ochraně osobních údajů, a to s přihlédnutím k okolnostem každého jednotlivého případu⁸⁷.
114. **V případě zjištění porušení předpisů mohou dozorové úřady uložit nápravná opatření, například nařídit správci, aby s ohledem na okolnosti daného případu přijali opatření k nápravě protiprávnosti počátečního zpracování.** Ta mohou zahrnovat například uložení pokuty, uložení dočasného omezení zpracování, výmaz části souboru údajů, který byl zpracován protiprávně, nebo, není-li to možné, v závislosti na daných skutečnostech a s ohledem na přiměřenost opatření nařízení výmazu celého souboru údajů používaného k vývoji modelu AI a/nebo výmazu modelu AI jako takového. Při posuzování přiměřenosti zamýšleného opatření mohou dozorové úřady zohlednit opatření, která může správce použít k nápravě protiprávnosti počátečního zpracování (např. opakování trénování).
115. EDPB rovněž zdůrazňuje, že pokud jsou osobní údaje zpracovávány protiprávně, mohou subjekty údajů požádat o výmaz svých osobních údajů za podmínek stanovených v článku 17 obecného nařízení o ochraně osobních údajů a že dozorové úřady mohou nařídit výmaz osobních údajů z moci úřední⁸⁸.
116. Při posuzování toho, zda je opatření vhodné, nezbytné a přiměřené, mohou dozorové úřady mimo jiné zvážit rizika, která z něho plynou pro subjekty údajů, závažnost porušení, technickou a finanční proveditelnost opatření, jakož i objem dotčených osobních údajů.
117. V neposlední řadě EDPB připomíná, že opatřeními přijatými dozorovými úřady podle obecného nařízení o ochraně osobních údajů nejsou dotčena opatření přijatá příslušnými orgány podle aktu o AI a/nebo podle jiných platných právních rámců (jako jsou právní předpisy o občanskoprávní odpovědnosti).
118. V následujících oddílech se EDPB bude zabývat třemi scénáři, o kterých pojednává otázka č. 4 žádosti, přičemž rozdíly spočívají v tom, zda jsou osobní údaje zpracovávány za účelem vývoje modelu uchovávané v modelu a/nebo zda následné zpracování provádí tentýž nebo jiný správce.

⁸⁶ Možná bude nutné vzít v úvahu zvláštní vnitrostátní pravidla. Viz například článek 2-decies italského zákona o ochraně údajů (legislativní nařízení 196/2003), který stanoví, že údaje zpracovávány v rozporu s pravidly pro ochranu údajů nelze použít. Tím nejsou dotčeny jiné vnitrostátní právní rámce, jako jsou trestněprávní předpisy.

⁸⁷ V tomto ohledu viz 129. bod odůvodnění obecného nařízení o ochraně osobních údajů, jakož i rozsudek SDEU ze dne 26. září 2024, věc C-768–21, *TR proti Land Hessen* (ECLI:EU:C:2024:785), bod 37; rozsudek SDEU ze dne 7. prosince 2023, spojené věci C-26/22 a C-64/22, *SCHUFA Holding (Libération de reliquat de dette)* (ECLI:EU:C:2023:958), bod 57; a rozsudek SDEU ze dne 14. března 2024, věc C-46/23, *Újpesti Polgármesteri Hivatal* (ECLI:EU:C:2024:239), bod 34.

⁸⁸ V tomto ohledu viz stanovisko EDPB č. 39/2021 k otázce, zda by čl. 58 odst. 2 písm. g) obecného nařízení o ochraně osobních údajů mohl sloužit jako právní základ pro to, aby dozorový úřad mohl z moci úřední nařídit výmaz osobních údajů v situaci, kdy subjekt údajů takovou žádost nepodal, bod 28. V této souvislosti viz rovněž rozsudek SDEU ze dne 14. března 2024, věc C-46/23, *Újpesti Polgármesteri Hivatal* (ECLI:EU:C:2024:239), bod 42.

3.4.1 Scénář č. 1. Správce protiprávně zpracovává osobní údaje za účelem vývoje modelu, osobní údaje jsou uchovávány v modelu a následně zpracovávány stejným správcem (například v souvislosti se zavedením modelu)

119. Tento scénář se týká otázky č. 4 bodu i) žádosti v situaci, kdy správce protiprávně zpracovává osobní údaje (tj. nedodržel čl. 5 odst. 1 písm. a) a článek 6 obecného nařízení o ochraně osobních údajů) za účelem vývoje modelu AI, přičemž tento model AI uchovává informace týkající se identifikované nebo identifikovatelné fyzické osoby, a není tedy anonymní. Osobní údaje jsou pak následně zpracovávány stejným správcem (například v souvislosti se zavedením modelu). V souvislosti s tímto scénářem EDPB předkládá následující úvahy.
120. Pravomoc dozorového úřadu uložit nápravná opatření týkající se počátečního zpracování (jak je vysvětleno v bodech 113, 114 a 115 výše) by v zásadě měla dopad na následné zpracování (např. pokud dozorový úřad nařídí správci vymazat osobní údaje, které byly zpracovány protiprávně, tato nápravná opatření by správci neumožnila následně zpracovávat osobní údaje, na které se vztahovala opatření).
121. Pokud jde konkrétně o dopad protiprávního zpracování ve fázi vývoje na následné zpracování (například ve fázi zavádění), EDPB připomíná, že je povinností dozorových úřadů, aby provedly analýzu jednotlivých případů, ve které se zohlední konkrétní okolnosti každého případu.
122. **Otázky, zda fáze vývoje a fáze zavádění zahrnují samostatné účely (a představují tak samostatné činnosti zpracování) a do jaké míry ovlivňuje neexistence právního základu pro počáteční činnost zpracování zákonnost následného zpracování, by měly být posuzovány případ od případu v závislosti na kontextu případu.**
123. Například se zvláštním ohledem na právní základ vycházející z čl. 6 odst. 1 písm. f) obecného nařízení o ochraně osobních údajů, pokud je následné zpracování založeno na oprávněném zájmu, by při posouzení oprávněného zájmu měla být zohledněna skutečnost, že počáteční zpracování bylo protiprávní (např. pokud jde o rizika pro subjekty údajů nebo skutečnost, že subjekty údajů nemusí takové následné zpracování očekávat). V těchto případech může mít protiprávnost zpracování ve fázi vývoje vliv na zákonnost následného zpracování.

3.4.2 Scénář č. 2. Správce protiprávně zpracovává osobní údaje za účelem vývoje modelu, osobní údaje jsou uchovávány v modelu a zpracovávány jiným správcem v souvislosti se zavedením modelu

124. Tento scénář se týká otázky č. 4 bodu i) žádosti. Liší se od scénáře č. 1 (viz oddíl 3.4.1 tohoto stanoviska), neboť osobní údaje jsou následně zpracovávány jiným správcem v souvislosti se zaváděním modelu AI.
125. EDPB připomíná, že zjištění úloh přidělených těmto různým aktérům v rámci ochrany údajů je zásadním krokem k určení toho, které povinnosti podle obecného nařízení o ochraně osobních údajů se uplatní a kdo je za tyto povinnosti odpovědný, a že při posuzování povinností jednotlivých stran podle obecného nařízení o ochraně osobních údajů by měly být rovněž zohledněny situace, kdy jsou správci společní. Níže uvedené připomínky by proto měly být považovány za obecné aspekty, které by měly dozorové úřady v příslušných případech zohlednit. V souvislosti s tímto scénářem č. 2 EDPB předkládá následující úvahy.
126. Zaprvé je třeba připomenout, že podle čl. 5 odst. 1 písm. a) ve spojení s čl. 5 odst. 2 obecného nařízení o ochraně osobních údajů by každý správce měl zajistit zákonnost zpracování, které provádí, a být schopen zákonnost zpracování doložit. Dozorové úřady by proto měly posoudit zákonnost zpracování

prováděného i) správcem, který původně vyvinul model AI; a ii) správcem, který získal model AI a sám zpracovává osobní údaje.

127. Zadruhé úvahy uvedené v bodech 113, 114 a 115 výše jsou relevantní i v tomto případě, pokud jde o pravomoc dozorových úřadů zasáhnout v souvislosti s počátečním zpracováním. V závislosti na okolnostech případu může být v této souvislosti relevantní také čl. 17 odst. 1 písm. d) (výmaz protiprávně zpracovaných údajů) a článek 19 (oznamovací povinnost ohledně opravy nebo výmazu osobních údajů nebo omezení zpracování) obecného nařízení o ochraně osobních údajů, například v souvislosti s oznámením, které by měl správce, který model vyvíjí, učinit vůči správci, který model zavádí.
128. Zatřetí možný dopad protiprávnosti počátečního zpracování na následné zpracování prováděné jiným správcem by dozorové úřady měly posuzovat případ od případu.
129. **Dozorové úřady by měly zohlednit, zda správce, který model zavádí, provedl náležité posouzení v rámci svých povinností týkajících se odpovědnosti⁸⁹ za doložení souladu s čl. 5 odst. 1 písm. a) a článkem 6 obecného nařízení o ochraně osobních údajů, aby se ujistil, že model AI nebyl vyvinut s využitím protiprávního zpracování osobních údajů.** Toto hodnocení ze strany dozorových úřadů by mělo zohlednit, zda správce posoudil některá kritéria z demonstrativního výčtu, jako je zdroj údajů, a to, zda při vývoji modelu AI došlo k porušení obecného nařízení o ochraně osobních údajů, zejména pokud to konstatoval dozorový úřad nebo soud, aby správce, který model zavádí, nemohl opomenout, že počáteční zpracování bylo protiprávní.
130. Správce by měl například zvážit, zda údaje pocházejí z porušení zabezpečení osobních údajů nebo zda zpracování bylo předmětem zjištění porušení předpisů, které konstatoval dozorový úřad nebo soud. **Míra posouzení ze strany správce a míra podrobností, kterou očekávají dozorové úřady, se mohou lišit v závislosti na různých faktorech, včetně druhu a míry rizik spojených se zpracováním v modelu AI během jeho zavádění ve vztahu k subjektům údajů, jejichž údaje byly použity při vývoji modelu.**
131. EDPB konstatuje, že akt o AI stanoví povinnost, aby poskytovatelé vysoce rizikových systémů AI vypracovali EU prohlášení o shodě⁹⁰, které uvádí, že příslušný systém AI je v souladu s právními předpisy EU o ochraně údajů⁹¹. EDPB konstatuje, že takové vlastní prohlášení nemusí představovat průkazné zjištění souladu s obecným nařízením o ochraně osobních údajů. Dozorové úřady je však mohou vzít v úvahu při zkoumání konkrétního modelu AI.
132. Tytéž úvahy uvedené v bodě 123 výše jsou relevantní i v tomto případě. Když dozorové úřady ověřují, zda a jak správce posoudil vhodnost oprávněného zájmu jako právního základu pro zpracování, které provádí, měla by být v rámci posouzení oprávněného zájmu brána v úvahu protiprávnost počátečního zpracování, například posouzením potenciálních rizik, která mohou vzniknout pro subjekty údajů, jejichž osobní údaje byly zpracovány protiprávně za účelem vývoje modelu. V rámci testu vyváženosti je třeba náležitě zvážit různá hlediska, ať už technické povahy (např. existenci filtrů nebo omezení přístupu zavedená během vývoje modelu, které následný správce nemůže obejít nebo ovlivnit a které by mohly zabránit přístupu k osobním údajům nebo jejich zveřejnění), nebo právní povahy (např. povahu a závažnost protiprávnosti původního zpracování).

⁸⁹ Čl. 5 odst. 2 a článek 24 obecného nařízení o ochraně osobních údajů.

⁹⁰ Čl. 16 písm. g) a článek 47 aktu o AI.

⁹¹ Příloha V bod 5 aktu o AI.

3.4.3 Scénář č. 3. Správce protiprávně zpracovává osobní údaje za účelem vývoje modelu, poté zajistí, aby byl model anonymizován, a to předtím, než stejný nebo jiný správce zahájí další zpracování osobních údajů v souvislosti se zaváděním

133. Tento scénář se týká otázky č. 4 bodu ii) žádosti a pojednává o případě, kdy správce protiprávně zpracovává osobní údaje za účelem vývoje modelu AI, ale činí tak způsobem, který zajišťuje, aby byly osobní údaje anonymizovány předtím, než tentýž nebo jiný správce zahájí další zpracování osobních údajů v souvislosti se zaváděním. Zprvu EDPB připomíná, že dozorové úřady jsou způsobilé a mají pravomoc zasáhnout, pokud jde o zpracování související s anonymizací modelu, jakož i o zpracování prováděné ve fázi vývoje. Dozorové úřady tedy mohou v závislosti na konkrétních okolnostech případu uložit nápravná opatření pro toto počáteční zpracování (jak je vysvětleno v bodech 113, 114 a 115 výše).
134. Pokud lze doložit, že následný provoz modelu AI nezahrnuje zpracování osobních údajů, má EDPB za to, že obecné nařízení o ochraně osobních údajů by se na něj nevztahovalo⁹². Protiprávnost počátečního zpracování by proto neměla mít vliv na následný provoz modelu. EDPB však zdůrazňuje, že pouhé tvrzení o anonymitě modelu nestačí k tomu, aby byl vyňat z působnosti obecného nařízení o ochraně osobních údajů, a upozorňuje, že dozorové úřady by jej měly individuálně v každém jednotlivém případě posoudit s přihlédnutím k úvahám, které uvedl EDPB v souvislosti s otázkou č. 1 žádosti.
135. **Pokud správci následně zpracovávají osobní údaje shromážděné během fáze zavádění poté, co byl model anonymizován, vztahuje se na tyto činnosti zpracování obecné nařízení o ochraně osobních údajů. V těchto případech, pokud jde o obecné nařízení o ochraně osobních údajů, by zákonnost zpracování prováděného ve fázi zavádění neměla být dotčena protiprávností počátečního zpracování.**

4 Závěrečné poznámky

136. Toto stanovisko je určeno všem dozorovým úřadům a bude zveřejněno podle čl. 64 odst. 5 písm. b) obecného nařízení o ochraně osobních údajů.

Za Evropský sbor pro ochranu osobních údajů
předsedkyně

Anu Talus

⁹² 26. bod odůvodnění obecného nařízení o ochraně osobních údajů.