SEDLAKOVA LEGAL

Applifting

Směrnice o možnostech užívání umělé inteligence

Pavel Čech
Sedlakova Legal s. r. o.
+420 733 555 958

Vratislav Kalenda & Prokop Simek
Applifting s. r. o.
+420 605 540 481

1. JAK PRACOVAT SE SMĚRNICÍ

1.1. Směrnice na poslední straně obsahuje checklist, který by měla odpovědná osoba vyplnit vždy před zavedením užívání nového nástroje umělé inteligence a dále vždy před změnou účelu, za kterým bude nástroj užíván.

1.2. Účelem směrnice je usnadnit odpovědné osobě rozhodování o tom, zda je zamýšlené využití nástroje umělé inteligence v pořádku. Směrnice však neobsahuje vyčerpávající výčet všech rizik a pravidel spojených s jejím užíváním, neboť je s ohledem na samotnou podstatu umělé inteligence nelze zcela bez výjimky předvídat.

2. DEFINICE

2.1. **Nástroj** je ChatGPT, Midjourney, deepL nebo jakýkoliv jiný nástroj, který umožňuje na základě uživatelem definovaných vstupů generovat výstupy, jako je například text, grafika, doporučení nebo predikce. Není důležité, zda je konkrétní nástroj cloudový nebo instalovaný, vyvinutý na míru nebo poskytovaný široké veřejnosti, ani zda je vyvinut pomocí strojového učení nebo jiné podobné techniky. Pravidla uvedená v této směrnici lze totiž použít na práci s jakýmkoliv inteligentním nástrojem, ať už využívá umělé inteligence či nikoliv.

2.2. **Odpovědná osoba** je manažer, technický ředitel (CTO), odborník na compliance nebo kdokoliv jiný, kdo má ve společnosti na starost užívání, bezpečnost nebo vývoj nástroje.

3. ZAKÁZANÉ OBLASTI

3.1. Je zakázáno používat nástroje, které:

a. využívají podprahových technik mimo vědomí osob nebo zranitelnosti určité skupiny osob v důsledku jejich věku nebo tělesného nebo mentálního postižení;

b. hodnotí nebo klasifikují důvěryhodnost osob na základě jejich sociálního chování nebo osobnostních vlastností (sociální kredit) ze strany orgánů veřejné moci nebo jejich jménem;

c. využívají biometrické identifikace na dálku „v reálném čase“ na veřejně přístupných místech pro účely prosazování práva, pokud to není nezbytně nutné pro cílené vyhledávání obětí trestných činů, prevenci bezpečnosti nebo teroristického útoku, nebo stíhání pachatelů trestného činu.

3.2. Výjimky připouštějící užívání nástrojů v zakázaných oblastech jsou uvedeny v návrhu Nařízení Evropského parlamentu a Rady, kterým se stanoví harmonizovaná pravidla pro umělou inteligenci (Aktu o umělé inteligenci) a mění určité legislativní akty Unie (dále jen **„Akt o umělé inteligenci“**).

4. VYSOCE RIZIKOVÉ OBLASTI

4.1. Následující odvětví a účely užívání nástrojů jsou považovány za vysoce rizikové:

a. vytváření deepfake nebo jiných výstupů, které mohou narušovat práva na ochranu osobnosti;

b. vzdělávání, odborná příprava, zaměstnanost, nábor, hodnocení výkonnosti a chování;

c. produkt, na který se vztahuje povinnost posouzení shody za účelem jeho uvedení na trh nebo do provozu, nebo který je určený k použití jako součást výrobku, na který se vztahují harmonizační právní předpisy Unie, jako například zdravotnické potřeby, vozidla, strojní zařízení, hračky, výtahy, rádiová zařízení, ochranné prostředky apod.;

d. řízení a provozování kritické infrastruktury (zejména silniční doprava, dodávky vody, plynu, tepla a elektřiny);

e. přístup k základním soukromým a veřejným službám a dávkám (hodnocení nároků na dávky a služby veřejné podpory, hodnocení úvěruschopnosti, vysílání nebo stanovení priority při vyslání zásahových služeb první reakce, včetně hasičů a lékařské pomoci);

f. vymáhání práva při použití donucovacími orgány (posouzení rizik protiprávního jednání, zjišťování emočního stavu, hodnocení spolehlivosti důkazů, profilování fyzických osob, analýz trestné činnosti), systémy určené na pomoc soudnímu orgánu při zkoumání a výkladu fakt a práva a při uplatňování práva a systémy použité v souvislostí s migrací, azylem a správou hraničních kontrol;

g. rozhodnutí, která mají významný dopad na lidský život nebo zdraví (včetně vývoje autonomních zbraní, které mohou rozhodovat o životě a smrti bez lidského zásahu) nebo soukromí.

4.2. Další příklady rizikových odvětví a účelů užívání nástrojů představují vysoce rizikové systémy AI dle Aktu o umělé inteligenci.

4.3. V případě užití nástroje ve vysoce rizikové oblasti je třeba důkladné zvážení implementace nástrojů a zevrubné posouzení nástrojů dle následujících článků směrnice.

5. BEZPEČNOST A DŮVĚRNOST

5.1. Před zahájením užívání nástroje odpovědná osoba posoudí:

a. **Potřebu školení zaměstnanců,** kteří budou používat nástroj nebo spravovat související data, aby rozuměli rizikům a nejlepším postupům v oblasti kybernetické bezpečnosti;

b. **Důvěryhodnost dodavatele nástroje,** například prostřednictvím referencí a zkušeností dodavatele v oboru;

c. **Zabezpečení dat,** zejména že nástroj nabízí dostatečná opatření, jako je šifrování při ukládání i přenosu nebo multifaktorové ověření.

5.2. Pokud má být nástroj používán ve spojení s velkým množstvím dat, důvěrnými daty nebo daty chráněnými právy duševního vlastnictví (autorské právo, databázová práva, obchodní tajemství apod.) zváží dále odpovědná osoba, zda by před zahájením užívání nástroje neměla být zajištěna:

a. **Certifikace dodavatele** v oblasti kybernetické bezpečnosti a ochrany dat (ISO 27001, SOC 2 nebo podobné standardy);

b. **Řízení přístupu,** přístup k nástroji by měl být omezen pouze na ty, kteří jej skutečně potřebují, a je třeba používat silná hesla;

c. **Pravidelné testování a revize,** pravidelné testování zabezpečení nástroje, včetně penetračních testů a revizí, aby bylo možné identifikovat a řešit zranitelnosti.;

d. **Plán reakce na incidenty,** tedy vypracovaný plán reakce na bezpečnostní incidenty související s nástrojem, který stanoví, jak by měla společnost reagovat na potenciální útoky nebo narušení zabezpečení.

6. OCHRANA OSOBNÍCH ÚDAJŮ

6.1. Oprávněná osoba zajistí:

a. **Minimální zpracování dat ve smyslu osobních údajů,** tedy usiluje o omezení zpracování osobních údajů na minimum. Do nástroje by měly být vkládány pouze nezbytně nutné osobní údaje;

b. **Anonymizace a pseudonymizace,** kdekoliv je to možné zajistí odpovědná osoba anonymizaci nebo pseudonymizaci osobních údajů před jejich zpracováním v nástroji;

c. **Zabezpečení osobních údajů,** tedy implementaci takových technických a organizačních opatření, aby nemohlo dojít k neoprávněnému nebo nahodilému přístupu k osobním údajům, k jejich změně, zničení či ztrátě, neoprávněným přenosům, k jejich jinému neoprávněnému zpracování, jakož i k jinému zneužití osobních údajů;

d. **Zpracovatelské podmínky**, pokud bude při užívání nástroje docházet ke zpracování osobních údajů, tak před zahájením takového zpracování společnost uzavře s provozovatelem nástroje zpracovatelskou smlouvu ve smyslu čl. 28 odst. 3 Nařízení Evropského parlamentu a Rady (EU) 2016/679 (obecné nařízení o ochraně osobních údajů);

e. **Transparentnost,** tedy poskytnutí jasných a srozumitelných informací subjektům údajů o tom, že jsou jejich osobní údaje nástrojem zpracovávány, o jaké osobní údaje se jedná, za jakým účelem je tak prováděno, na základě jakého právního základu a jaká jsou jejich práva v souvislosti se zpracováním.

6.2. V případě, že použití nástroje představuje významné riziko pro práva a svobody jednotlivců, zváží oprávněná osoba provedení posouzení dopadu na ochranu údajů (DPIA).

7. AUTORSKÁ PRÁVA A OCHRANA VSTUPŮ

7.1. Je zakázáno používat nástroj k vytváření výstupů, které mají být poskytovány zákazníkovi současně s poskytnutím určité úrovně práv duševního vlastnictví. Jedná se zejména o případy generovaných výstupů jako jsou grafické materiály nebo části počítačového kódu, u kterých je nezbytné zákazníkovi poskytnout:

a. Výhradní licenci nebo postoupení výkonu majetkových autorských práv;

b. Záruku vytvoření výstupu jakožto autorského díla (včetně zaměstnaneckého díla);

c. Dílo, které není založeno na původním díle třetí strany.

7.2. Při posuzování, zda je při užití nástroje možné zaručit požadovanou právní ochranu, odpovědná osoba dále posoudí smluvní podmínky užívání nástroje a podmínky smlouvy se zákazníkem, které se týkají požadovaných práv k poskytnutému výstupu.

7.3. Odpovědná osoba odpovídá za to, že uživatelé nástroje respektují práva duševního vlastnictví třetích stran a jsou poučeni o tom, že bez příslušného svolení (například uzavřené licenční smlouvy) nevkládají do nástroje:

a. Autorská díla, jako například grafická, hudební nebo textová díla, fotografie, počítačové programy nebo audiovizuální díla;

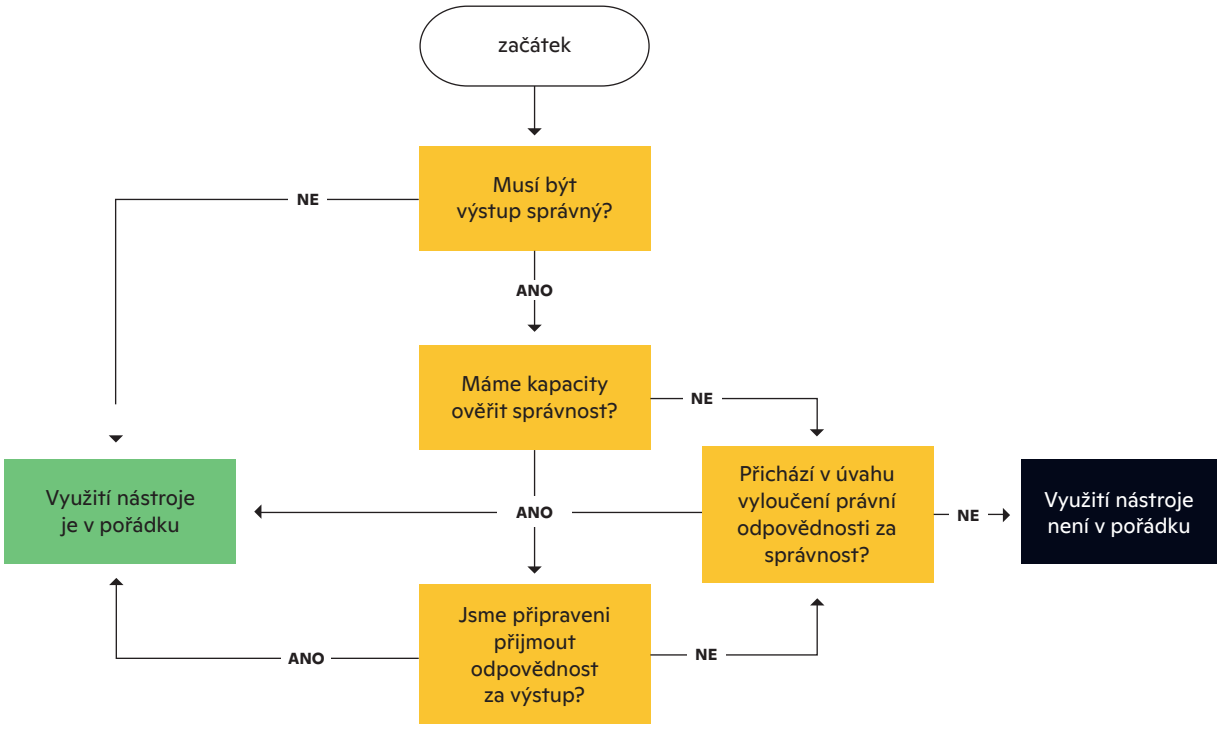
b. Databáze, zejména pokud jejich majitel musel vynaložit podstatné úsilí do jejich pořízení, ověření nebo předvedení obsahu;

c. Informace, které mohou představovat obchodní tajemství;

d. Jiné důvěrné informace, zejména jsou chráněny povinností mlčenlivosti, například údaje o zákaznících, obchodních partnerech, obchodní strategie, marketingové plány, interní dokumentace apod.

8. NESPRÁVNOST VÝSTUPU

8.1. Odpovědná osoba provede hodnocení rizik nesprávnosti výstupů nástroje podle následujícího diagramu:



Inspirace: Aleksandr Tiulkanov, https://tiulkanov.files.wordpress.com/2023/03/is-it-safe-to-use-chatgpt-for-your-task.pdf

8.2. Při rozhodování o tom, zda má společnost kapacity ověřit správnost výstupů nástroje, vezme odpovědná osoba v úvahu možnosti:

a. kontroly faktické správnosti údajů;

b. kontroly předsudků a diskriminačních vzorců z tréninkových dat;

c. kontroly podobnosti či shodnosti výstupu s některým z prvků tréninkových dat (riziko záměny výstupu za plagiát);

d. uživatelského proškolení, jak správně výstupy kontrolovat.

8.3. Při rozhodování o tom, zda je společnost připravena přijmout odpovědnost za výstup, dále odpovědná osoba posoudí:

a. pravděpodobnost vzniku újmy;

b. závažnost případné újmy.

8.4. Při rozhodování o tom, zda přichází v úvahu omezení právní odpovědnosti za výstup, odpovědná osoba posoudí, zda:

a. Právní předpisy umožňují omezení odpovědnosti za vady a/nebo újmu způsobenou nesprávností výstupu;

b. můžeme si (zejména z obchodního hlediska) dovolit omezení odpovědnosti vůči uživateli.

9. SMLUVNÍ PODMÍNKY UŽÍVÁNÍ NÁSTROJE

9.1. Odpovědná osoba zkontroluje, zda smluvní podmínky užívání nástroje neobsahují některé z následujících ujednání, která představují zmíněná rizika; v případě, že obsahují, odpovědná osoba zároveň posoudí, zda ujednání nebrání užívání nástroje za zamýšleným účelem nebo nepředstavují nepřijatelné riziko, kvůli kterému je nezbytné dojednat úpravy smluvních podmínek:

a. Vstupy zadané do nástroje mohou být použity za účelem jeho zlepšování. V případě takového smluvního ujednání hrozí zvýšené riziko zneužití vstupů, jelikož mohou být zpřístupněny třetím stranám.
b. Zákaz komerčního užití výstupů. Komerční užití bývá často podmíněno zakoupením (vyšší) úrovně předplatného. Výstupy nástroje přitom mohou být technicky označeny, takže Vaše případné nedodržení licenčních podmínek může být snadno odhaleno.
c. Licence k výstupům nástroje je poskytována provozovateli. Pokud smluvní podmínky obsahují ujednání o poskytnutí licenčních oprávnění ve prospěch provozovatele nástroje, opět hrozí zvýšené riziko, že generované výstupy z nástroje mohou užívat třetí strany.

9.2. Odpovědná osoba dále zkontroluje, zda smluvní podmínky obsahují následující záruky pro užívání nástroje, a pokud je neobsahují, tak zváží možnosti dojednání úprav smluvních podmínek:

a. Možnost migrace a exportu dat z nástroje;

b. SLA na dostupnost nástroje (například 99,9 % času v měsíci), případně reakční doby pro vyřešení výpadku, v každém případě také existence nápravných opatření (smluvní pokuty, slevy) v případě jejich nedodržení.

10. VÝVOJ NÁSTROJE NA MÍRU

10.1. Před zahájením vývoje vlastního nástroje odpovědná osoba zváží, jaké funkční požadavky budou na nástroj kladeny, tak aby byl:
a. transparentní;

b. přesný;

c. spolehlivý;

d. bezpečný.

10.2. Odpovědná osoba dále posoudí:

a. Zda vývoj nebo užívání nástroje není upraven zvláštní právní regulací, zejména zda se nejedná o systém spadající pod některou ze zakázaných oblastí dle článku 3 této směrnice nebo vysoce rizikových oblastí dle článku 4 této směrnice;

b. Zda je dostatečně zajištěno, aby byla použitá tréninková data „čistá", zejména z pohledu práv duševního vlastnictví a minimalizace osobních údajů;

c. Jakou dokumentaci nástroje by bylo vhodné v průběhu vývoje zpracovávat;

d. Zda není vhodné zavést nástroj, který by v rámci celého životního cyklu nástroje sloužil k identifikaci, analýze a hodnocení rizik souvisejících s jeho vývojem a užíváním, stejně jako k přijetí vhodných opatření k jejich řízení.

10.3. Před objednáním takového vývoje u třetí strany, odpovědná osoba dále zváží:

a. Jaké jsou záruky právní nezávadnosti tréninkových dat, zejména že použitá tréninková data neobsahují materiály chráněné autorským právem a že jsou garantována řádná oprávnění k jejich použití.

b. Jaká bude odpovědnost dodavatele (třetí strany) za kvalitu a správnost výstupů nástroje?

c. Kdo bude provozovatelem vyvinutého nástroje (zvažte mimo jiné otázky odpovědnosti za provozování nástroje a dosažení souladu s právními předpisy).

d. Jestli je dostatečně zabráněno riziku závislosti na vybraném dodavateli, jeho technologiích, licenčních podmínkách a podpoře.

Checklist

#	Otázka	Doporučení
1.	**ÚVODNÍ DOTAZY**	
1.1.	Umožňuje nástroj generovat výstupy, jako je například text, grafika, doporučení nebo predikce?	Pokud ano, je potřeba posoudit další otázky z tohoto checklistu.
1.2.	Spadá nástroj do zakázané oblasti (viz článek 3.1. směrnice)?	Pokud ano, nedoporučujeme nástroj využívat.
		Pokud ne, je potřeba posoudit další otázky z tohoto checklistu.
1.3.	Spadá nástroj do některé z vysoce rizikových oblastí (viz článek 4 směrnice)?	Pokud ano, je před zahájením vývoje nebo užívání nástroje potřeba provést důkladnou právní analýzu.
		Pokud ne, doporučujeme před zahájením vývoje nebo užívání nástroje posouzení dle bodu 2. checklistu.

#	Otázka	Doporučení
2.	**POSOUZENÍ BEZPEČNOSTI A DŮVĚRNOSTI**	
2.1.	Proběhlo školení zaměstnanců?	Pokud ne, implementace nástroje může přinést bezpečnostní riziko a nedoporučujeme ji.
2.2.	Byla posouzena důvěryhodnost dodavatele nástroje?	Pokud ne, implementace nástroje může přinést bezpečnostní riziko a nedoporučujeme ji.
2.3.	Nabízí nástroj dostatečné zabezpečení Vašich dat?	Pokud ne, implementace nástroje může přinést bezpečnostní riziko a nedoporučujeme ji.
2.4.	Má být nástroj používán ve spojení s velkým množstvím dat, důvěrnými daty nebo daty chráněnými právy duševního vlastnictví (autorské právo, databázová práva, obchodní tajemství apod.)?	Pokud ano, pokračujte k následující otázce tohoto checklistu.
		Pokud ne, pokračujte k bodu 3. checklistu.
2.5.	Provedli jste certifikaci dodavatele v oblasti kybernetické bezpečnosti a ochrany dat (ISO 27001, SOC 2 nebo podobné standardy)?	Pokud ano, pokračujte k následující otázce tohoto checklistu.
		Pokud ne, implementace nástroje může přinést bezpečnostní riziko a nedoporučujeme ji.

2.6.	Má k nástroji přístup pouze ten, kdo jej skutečně potřebuje a používá k nástroji silná hesla?	Pokud ano, pokračujte k následující otázce tohoto checklistu.
		Pokud ne, implementace nástroje může přinést bezpečnostní riziko a nedoporučujeme ji.
2.7.	Je zabezpečení nástroje pravidelně testováno, včetně penetračních testů a revizí, aby bylo možné identifikovat a řešit zranitelnosti?	Pokud ano, pokračujte k následující otázce tohoto checklistu.
		Pokud ne, implementace nástroje může přinést bezpečnostní riziko a nedoporučujeme ji.
2.8.	Máte vypracovaný plán reakce na bezpečnostní incidenty související s nástrojem, který stanoví, jak by měla společnost reagovat na potenciální útoky nebo narušení zabezpečení?	Pokud ano, pokračujte k následující otázce tohoto checklistu.
		Pokud ne, implementace nástroje může přinést bezpečnostní riziko a nedoporučujeme ji.

#	Otázka	Doporučení
3.	**OCHRANA OSOBNÍCH ÚDAJŮ**	
3.1	Máte zajištěno, aby byly do nástroje vkládány pouze nezbytně nutné osobní údaje a byly anonymizovány, kdekoli je to nutné?	Pokud ano, pokračujte k následující otázce tohoto checklistu.
		Pokud ne, doporučujeme přehodnotit využití nástroje.
3.2.	Máte osobní údaje řádně zabezpečeny?	Pokud ano, pokračujte k následující otázce tohoto checklistu.
		Pokud ne, doporučujeme přehodnotit využití nástroje.
3.3.	V případě, že při užívání nástroje dochází ke zpracování osobních údajů, máte uzavřenou zpracovatelskou smlouvu s provozovatelem nástroje?	Pokud ano, pokračujte k následující otázce tohoto checklistu.
		Pokud ne, doporučujeme přehodnotit využití nástroje.
3.4.	Poskytujete subjektům údajů jasné a srozumitelné informace o tom, že jsou jejich osobní údaje nástrojem zpracovávány, o jaké osobní údaje se jedná, za jakým účelem je tak prováděno, na základě jakého právního základu a jaká jsou jejich práva v souvislosti se zpracováním?	Pokud ano, pokračujte k následující otázce tohoto checklistu.
		Pokud ne, doporučujeme přehodnotit využití nástroje.

3.5.	Představuje použití nástroje významné riziko pro práva a svobody jednotlivců?	Pokud ano, zvažte provedení posouzení dopadu na ochranu údajů (DPIA).
		Pokud ne, pokračujte k bodu 4. checklistu.

#	Otázka	Doporučení
4.	**AUTORSKÁ PRÁVA**	
4.1.	Používáte nástroj k vytváření výstupů (jako jsou grafické materiály nebo části počítačového kódu), ke kterým je nezbytné zákazníkovi poskytnout práva duševního vlastnictví?	Pokud ano, pokračujte k následující otázce tohoto checklistu.
		Pokud ne, pokračujte k bodu 5. checklistu.
4.2.	Posoudili jste, zda je při užití nástroje možné smluvně zaručit požadovanou právní ochranu?	Pokud ano, pokračujte k následující otázce tohoto checklistu.
		Pokud ne, doporučujeme přehodnotit využití nástroje.
4.3.	Máte zajištěno, aby uživatelé nástroje respektovali práva duševního vlastnictví třetích stran a jsou náležitě poučeni o tom, co nástroje v tomto smyslu nemají vkládat?	Pokud ano, pokračujte k bodu 5. checklistu.
		Pokud ne, doporučujeme přehodnotit využití nástroje.

#	Otázka	Doporučení
5.	**ZHODNOCENÍ RIZIK NESPRÁVNOSTI VÝSTUPU**	
5.1.	Zhodnotili jste riziko nesprávnosti podle diagramu v článku 8.1 směrnice?	Pokud ne, doporučujeme přehodnotit využití nástroje.
		Pokud ano, pokračujte k bodu 6. checklistu.

#	Otázka	Doporučení
6.	**SMLUVNÍ PODMÍNKY UŽÍVÁNÍ NÁSTROJE**	
6.1.	Umožňují smluvní podmínky použití vašich vstupů za účelem jeho zlepšování?	Pokud ano, doporučujeme přehodnotit využití nástroje.
6.2.	Umožňují smluvní podmínky zamýšlené užití (například komerční užití, zpřístupnění výstupů třetím stranám)?	Pokud ne, doporučujeme přehodnotit využití nástroje.
6.3.	Poskytují smluvní podmínky provozovateli nástroje licenci k užívání vašich výstupů?	Pokud ano, doporučujeme přehodnotit využití nástroje.
6.4.	Umožňují smluvní podmínky možnost migrace a exportu dat z nástroje?	Pokud ne, doporučujeme přehodnotit využití nástroje.
6.5.	Máte ujednané SLA na dostupnost nástroje?	Pokud ne, doporučujeme přehodnotit využití nástroje.

#	Otázka	Doporučení
7.	**VYVÍJÍTE VLASTNÍ NÁSTROJ?**	
7.1.	Zvážili jste, jaké funkční požadavky budou na nástroj kladeny, tak aby byl transparentní, přesný, spolehlivý a bezpečný?	Pokud ano, pokračujte k následující otázce tohoto checklistu.
		Pokud ne, doporučujeme přehodnotit vývoj nástroje.
7.2.	Budou použitá tréninková data „čistá“, zejména z pohledu práv duševního vlastnictví a minimalizace osobních údajů?	Pokud ano, pokračujte k následující otázce tohoto checklistu.
		Pokud ne, vraťte se k bodům 3 a 4 tohoto checklistu.
7.3.	Posoudili jste, jakou dokumentaci nástroje by bylo vhodné v průběhu vývoje zpracovávat?	Pokud ano, pokračujte k následující otázce tohoto checklistu.
		Pokud ne, doporučujeme přehodnotit vývoj nástroje.

7.4.	Posoudili jste, zda není vhodné zavést nástroj, který by v rámci celého životního cyklu nástroje sloužil k identifikaci, analýze a hodnocení rizik souvisejících s jeho vývojem a užíváním, stejně jako k přijetí vhodných opatření k jejich řízení?	Pokud ano, pokračujte k následující otázce tohoto checklistu.
		Pokud ne, doporučujeme přehodnotit vývoj nástroje.
7.5.	Chcete si objednat vývoj nástroje u třetí strany?	Pokud ano, pokračujte k následující otázce tohoto checklistu.
		Pokud ne, vývoj nástroje můžete zahájit.
7.6.	Ověřili jste si, jaké jsou záruky právní nezávadnosti tréninkových dat, zejména že použitá tréninková data neobsahují materiály chráněné autorským právem a že jsou garantována řádná oprávnění k jejich použití?	Pokud ano, pokračujte k následující otázce tohoto checklistu.
		Pokud ne, doporučujeme přehodnotit vývoj nástroje třetí stranou.
7.7.	Ověřili jste si, jaká bude odpovědnost dodavatele (třetí strany) za kvalitu a správnost výstupů nástroje?	Pokud ano, pokračujte k následující otázce tohoto checklistu.
		Pokud ne, doporučujeme přehodnotit vývoj nástroje třetí stranou.
7.8.	Máte ošetřené veškeré otázky týkající se provozovatele vyvinutého nástroje (ve smyslu odpovědnosti za provozování nástroje a dosažení souladu s právními předpisy)?	Pokud ano, pokračujte k následující otázce tohoto checklistu.
		Pokud ne, doporučujeme přehodnotit vývoj nástroje třetí stranou.
7.9.	Zvážili jste, jestli je dostatečně zabráněno riziku závislosti na vybraném dodavateli, jeho technologiích, licenčních podmínkách a podpoře?	Pokud ano, vývoj nástroje můžete zahájit.
		Pokud ne, doporučujeme přehodnotit vývoj nástroje třetí stranou.