



Procurement of AI Community

● PUBLIC BUYERS COMMUNITY

Návrh štandardných zmluvných doložiek pre obstarávanie umelej inteligencie verejnými organizáciami, verzia zo septembra 2023 – zjednodušená verzia

DRAFT– Non High Risk version

Vyhlasenie o odmietnutí zodpovednosti

Toto je návrh dokumentu, ktorý slúži len ako podklad na diskusiu s cieľom získať úvodnú spätnú väzbu od zainteresovaných strán. Tento dokument vypracoval Jeroen Naves (Pels Rijcken). Nejde o oficiálny dokument EÚ a za žiadnych okolností sa nemôže považovať za vyjadrenie oficiálneho stanoviska Európskej komisie. Európska komisia ani žiadna osoba konajúca v mene Komisie nie je zodpovedná za možné použitie tohto dokumentu. Tento dokument ešte stále nie je dokončený. Na základe tohto dokumentu nemôžu byť odvodené žiadne práva.

Úvodné poznámky

Tieto štandardné zmluvné doložky boli vypracované pre verejné organizácie, ktoré chcú obstarávať systém umelej inteligencie vyvinutý externým dodávateľom. Tieto štandardné doložky vychádzajú zo štandardných doložiek pre obstarávanie algoritmických systémov, ktoré vypracovalo mesto Amsterdam v roku 2018 (<https://www.amsterdam.nl/innovatie/digitalisering-technologie/algoritmen-ai/contractual-terms-for-algorithms/>).

Predstavené štandardné zmluvné doložky vychádzajú do veľkej miery z požiadaviek a povinností týkajúcich sa vysokorizikových systémov umelej inteligencie, ktoré sú zahrnuté v hlave III návrhu nariadenia o umelej inteligencii* (ďalej len „akt o umelej inteligencii“). Tento návrh je predmetom prebiehajúcich rokovaní, preto sa doložky budú musieť zrevidovať s cieľom zohľadniť všetky vykonané zmeny a plne ich zosúladiť s konečným znením nariadenia, ktoré prijme Rada a Európsky parlament.

Vzhľadom na to, že navrhovaný akt o umelej inteligencii je stále predmetom rokovaní, verejné organizácie, ktoré sa rozhodnú použiť štandardné zmluvné doložky, tak môžu urobiť na dobrovoľnom základe a v konkrétnych prípadoch posúdiť, či sú jednotlivé oddiely týchto štandardných zmluvných doložiek dostatočné a primerané na obstaranie konkrétneho systému umelej inteligencie. Úplná verzia štandardných zmluvných doložiek je zameraná predovšetkým na systémy umelej inteligencie, ktoré sú v zmysle článku 6 klasifikované ako „vysokorizikové“ a sú uvedené v rámci jednej z oblastí, na ktoré sa vzťahujú prílohy II a III navrhovaného aktu o umelej inteligencii.

V prípade umelej inteligencie, ktorá nie je vysokoriziková, nie je uplatňovanie týchto požiadaviek podľa aktu o umelej inteligencii povinné, ale odporúča sa, a to s cieľom zvýšiť dôveryhodnosť aplikácií umelej inteligencie, ktoré obstarávajú verejné organizácie. Táto zjednodušená verzia štandardných zmluvných doložiek je zameraná predovšetkým na systémy umelej inteligencie, ktoré nie sú vysokorizikové.

V prípadoch, keď je to v závislosti od vplyvu systému na jednotlivcov a spoločnosť primerané a odôvodnené, môžu verejné organizácie rozšíriť uplatňovanie týchto doložiek, a to buď ich úplnej, alebo tejto zjednodušenej verzie, aj na iné algoritmické systémy, ktoré nemusia byť nevyhnutne kvalifikované ako „umelá inteligencia“, s cieľom zahrnúť aj jednoduchšie softvérové systémy založené na pravidlách, keďže pri ich používaní vo verejnom sektore môže byť v niektorých prípadoch takisto potrebná väčšia zodpovednosť, kontrola a transparentnosť.

Štandardné zmluvné doložky obsahujú len ustanovenia špecifické pre systémy umelej inteligencie a týkajúce sa záležitostí, na ktoré sa vzťahuje navrhovaný akt o umelej inteligencii, a preto nezahŕňajú iné povinnosti ani požiadavky, ktoré môžu vyplývať z príslušných platných právnych predpisov, ako je napríklad všeobecné nariadenie o ochrane údajov. Tieto štandardné zmluvné doložky navyše neobsahujú úplnú zmluvnú dohodu. Tieto štandardné zmluvné doložky napríklad neobsahujú žiadne podmienky týkajúce sa duševného vlastníctva, prijatia, platby, časoch dodania, uplatniteľného práva či zodpovednosti. Štandardné zmluvné doložky sú vypracované takým spôsobom, aby sa mohli pripojiť ako príloha k dohode, v ktorej sa takéto záležitosti stanovujú.

* Návrh nariadenia Európskeho parlamentu a Rady, ktorým sa stanovujú harmonizované pravidlá v oblasti umelej inteligencie a menia niektoré legislatívne akty Únie, COM(2021) 206 final.

Oddiel A – Vymedzenie pojmov

Article 1 Vymedzenie pojmov

1.1. Pojmy používané v týchto doložkách budú mať význam vymedzený v tomto článku:

- dohoda: celá dohoda, ktorej neoddeliteľnou súčasťou sú doložky vo forme prílohy,
- systém umelej inteligencie: systém (systémy) umelej inteligencie, ktoré sú uvedené v **prílohe A**, vrátane všetkých ich nových verzií,
- doložky: tieto štandardné zmluvné doložky pre obstarávanie umelej inteligencie verejnými organizáciami,
- súbory údajov verejnej organizácie: súbory údajov (alebo ich časti), ktoré i) poskytla verejná organizácia dodávateľovi podľa dohody alebo ii) sa majú vytvoriť alebo zhromaždiť ako súčasť dohody, a to vrátane všetkých upravených alebo rozšírených verzií súborov údajov uvedených v bodoch i) a ii) (napríklad z dôvodu anotácie, označovania, čistenia, obohacovania alebo agregácie),
- súbory údajov: všetky súbory údajov použité pri vývoji systému umelej inteligencie vrátane súboru údajov alebo súborov údajov opísaných v **prílohe B**,
- dodanie: čas, keď dodávateľ informuje verejnú organizáciu, že systém umelej inteligencie spĺňa všetky dohodnuté podmienky a je pripravený na použitie,
- zamýšľaný účel: použitie systému umelej inteligencie, ktoré určila verejná organizácia, vrátane osobitného kontextu a podmienok používania, ako sa uvádza v prílohe B, informáciách od dodávateľa v návode na použitie, v propagačných alebo predajných materiáloch a vo vyhláseniach, ako aj v technickej dokumentácii,
- logicky predvídateľné nesprávne použitie: také použitie systému umelej inteligencie, ktoré nie je v súlade so zamýšľaným účelom, ale ktoré môže byť výsledkom logicky predvídateľného ľudského správania alebo interakcie s inými systémami,
- podstatná zmena: zmena systému umelej inteligencie po jeho dodaní, ktorá ovplyvňuje súlad systému umelej inteligencie s požiadavkami stanovenými v týchto doložkách alebo vedie k zmene zamýšľaného účelu,
- dodávateľ: fyzická alebo právnická osoba, orgán verejnej moci, agentúra alebo iný orgán, ktorý dodáva systém umelej inteligencie verejnej organizácii podľa dohody,
- súbory údajov dodávateľa a súbory údajov tretej strany: súbory údajov (alebo ich časti), ktoré sa nepovažujú za súbory údajov verejnej organizácie.

Oddiel B – Základné požiadavky v súvislosti so systémom umelej inteligencie

Article 2 Systém riadenia rizík

- 2.1. Dodávateľ zaistí, aby sa pred dodaním systému umelej inteligencie v súvislosti s ním zriadil a zaviedol systém riadenia rizík.
- 2.2. Systém riadenia rizík zahŕňa minimálne tieto kroky:
- a. identifikáciu, odhad a hodnotenie známych a logicky predvídateľných rizík pre zdravie, bezpečnosť a základné práva Európskej únie, ktoré by mohli vzniknúť vzhľadom na zamýšľaný účel systému umelej inteligencie a logicky predvídateľné nesprávne použitie;

- b. hodnotenie ďalších možných vznikajúcich rizík;
 - c. prijatie primeraných a cielených opatrení na riadenie rizík navrhnutých na riešenie rizík identifikovaných podľa písmen a) a b) tohto bodu v súlade s ustanoveniami ďalších bodov.
- 2.3. Opatrenia na riadenie rizík uvedené v bode 2.2 písm. c) musia byť také, aby dodávateľ príslušné zvyškové riziká spojené s jednotlivými nebezpečenstvami, ako aj celkové zvyškové riziko systému umelej inteligencie odôvodnene považoval za prijateľné za predpokladu, že systém umelej inteligencie sa používa v súlade so zamýšľaným účelom alebo za podmienok logicky predvídateľného nesprávneho použitia.
- 2.4. Pri určovaní najvhodnejších opatrení na riadenie rizík uvedených v bode 2.2 písm. c) sa zabezpečí:
- a. odstránenie alebo obmedzenie identifikovaných rizík v najvyššej technicky dosiahnuteľnej miere prostredníctvom primeranej koncepcie a vývoja systému umelej inteligencie;
 - b. prípadné zavedenie primeraných zmierňujúcich a kontrolných opatrení v súvislosti s rizikami, ktoré nemožno odstrániť;
 - c. poskytovanie primeraných informácií verejnej organizácii.
- 2.5. Dodávateľ zaistí, aby sa systém umelej inteligencie pred dodaním otestoval s cieľom overiť, či je v súlade s doložkami a či sú opatrenia na riadenie rizík uvedené v bode 2.2 písm. c) vzhľadom na zamýšľaný účel a logicky predvídateľné nesprávne použitie účinné. Ak to verejná organizácia vyžaduje, dodávateľ je povinný testovať systém umelej inteligencie v prostredí verejnej organizácie.
- 2.6. Všetky identifikované riziká, prijaté opatrenia a testy vykonané v súvislosti s dodržiavaním tohto článku musí dodávateľ zdokumentovať. Dodávateľ musí túto dokumentáciu sprístupniť verejnej organizácii najneskôr v čase dodania systému umelej inteligencie. Táto dokumentácia môže byť súčasťou technickej dokumentácie a/alebo návodu na použitie.
- 2.7. Systém riadenia rizík sa chápe ako nepretržitý a iteratívny proces počas celého trvania dohody. Po dodaní systému umelej inteligencie musí preto dodávateľ:
- a. pravidelne preskúmať a aktualizovať proces riadenia rizík s cieľom zabezpečiť jeho nepretržitú účinnosť;
 - b. priebežne aktualizovať dokumentáciu opísanú v bode 2.6 a
 - c. bezodkladne sprístupňovať každú novú verziu dokumentácie opísanej v bode 2.6 verejnej organizácii.
- 2.8. Ak sa to odôvodnene vyžaduje na riadne vykonávanie systému riadenia rizík dodávateľom, verejná organizácia poskytne dodávateľovi na vyžiadanie informácie, pokiaľ nemajú dôverný charakter.
- 2.9. **<Nepovinné>** Ak používanie systému umelej inteligencie zo strany verejnej organizácie presahuje obdobie platnosti dohody, pri skončení platnosti dohody poskytne dodávateľ verejnej organizácii informácie potrebné na to, aby mohla systém riadenia rizík udržiavať sama.

Article 3 < Článok 3 je relevantný len pre systémy umelej inteligencie, ktoré využívajú techniky zahŕňajúce tréning modelov s údajmi. V článku 3 sa predpokladá, že dodávateľ (alebo jeho subdodávateľia) má (majú) plný prístup k súborom

údajov. Ak sú súbory údajov uchovávané výlučne verejnou organizáciou, je nevyhnutné uzavrieť iné dojednania.> Údaje a správa údajov

- 3.1. Dodávateľ zaistí to, že súbory údajov použité pri vývoji systému umelej inteligencie vrátane tréningu, validácie a testovania podliehali a podliehajú správe údajov, ktorá je primeraná pre kontext používania, ako aj zamýšľaný účel systému umelej inteligencie. Tieto opatrenia sa týkajú najmä:
- transparentnosti, pokiaľ ide o pôvodný účel zberu údajov;
 - príslušných rozhodnutí o koncepčných riešeniach;
 - postupov zberu údajov;
 - prípravy údajov na operácie spracovania, ako je anotácia, označovanie, čistenie, obohacovanie a agregácia;
 - formulovania relevantných predpokladov, najmä pokiaľ ide o informácie, ktoré majú údaje merať a reprezentovať;
 - preskúmania z hľadiska možných skreslení, ktoré by mohli ovplyvniť zdravie a bezpečnosť fyzických osôb alebo viesť k diskriminácii, ktorá je zakázaná právnymi predpismi Európskej únie;
 - primeraných opatrení na odhaľovanie a zmierňovanie možných skreslení, ako aj predchádzanie takýmto skresleniam;
 - identifikácie relevantných medzier alebo nedostatkov v údajoch, ktoré zabraňujú súladu s týmito doložkami, a spôsobu, akým možno tieto medzery a nedostatky odstrániť.
- 3.2. Dodávateľ zaistí, aby súbory údajov použité pri vývoji systému umelej inteligencie boli relevantné, reprezentatívne, v najlepšej možnej miere bezchybné a vzhľadom na zamýšľaný účel systému čo najúplnejšie. Dodávateľ zaistí, aby súbory údajov mali primerané štatistické vlastnosti, a to prípadne aj pokiaľ ide o osoby alebo skupiny osôb, v prípade ktorých sa má systém umelej inteligencie používať. Tieto charakteristiky súborov údajov musia byť splnené na úrovni jednotlivých súborov údajov alebo ich kombinácie.
- 3.3. Dodávateľ zaistí, aby v súboroch údajov použitých pri vývoji systému umelej inteligencie boli v rozsahu vyžadovanom vzhľadom na zamýšľaný účel alebo logicky predvídateľné nesprávne použitie zohľadnené vlastnosti alebo prvky, ktoré sú špecifické pre konkrétne geografické, kontextové, behaviorálne alebo funkčné podmienky, v ktorých sa má systém umelej inteligencie používať.
- 3.4. Povinnosti podľa tohto článku sa nevzťahujú iba na vývoj systému umelej inteligencie pred dodaním, ale aj na akékoľvek použitie súborov údajov dodávateľom, ktoré môže ovplyvniť fungovanie systému umelej inteligencie kedykoľvek počas obdobia platnosti dohody.

Article 4 Technická dokumentácia a návod na použitie

- 4.1. Dodanie systému umelej inteligencie dodávateľom zahŕňa odovzdanie technickej dokumentácie a návodu na použitie.
- 4.2. Technická dokumentácia musí verejnej organizácii alebo tretej strane umožniť posúdiť súlad systému umelej inteligencie s ustanoveniami požiadaviek stanovených v týchto doložkách a spĺňať aspoň podmienky opísané v **prílohe C**.

- 4.3. Návod na použitie obsahuje stručné, úplné, správne a jasné informácie, ktoré sú pre verejnú organizáciu relevantné, prístupné a zrozumiteľné. Návod na použitie musí spĺňať aspoň podmienky opísané v **prílohe D**.
- 4.4. Dodávateľ musí túto dokumentáciu aktualizovať prinajmenšom pri každej podstatnej zmene počas obdobia platnosti dohody a následne ju sprístupniť verejnej organizácii.
- 4.5. **<nepovinné>** Technická dokumentácia a návod na použitie musia byť vypracované v anglickom jazyku.
- 4.6. **<nepovinné>** Bez toho, aby boli dotknuté ustanovenia článkov 6 a 10, má verejná organizácia právo urobiť si z technickej dokumentácie a návodu na použitie kópie v rozsahu potrebnom na interné použitie v rámci štruktúry verejnej organizácie.

Article 5 Vedenie záznamov

- 5.1. Dodávateľ zaistí to, že systém umelej inteligencie bol a je koncipovaný a vyvinutý tak, aby bol počas svojej prevádzky schopný automaticky zaznamenávať udalosti („logy“). Tieto schopnosti logovania musia byť v súlade so špičkovou technológiou a s prípadnými uznávanými normami alebo spoločnými špecifikáciami. **<Nepovinné: pridajte konkrétnu normu, ak je k dispozícii>**
- 5.2. Schopnosťami logovania sa počas celého životného cyklu systému umelej inteligencie zabezpečí úroveň vysledovateľnosti jeho fungovania, ktorá je primeraná zamýšľanému účelu systému a logicky predvídateľnému nesprávne použitiu. Tieto schopnosti umožnia predovšetkým zaznamenávanie udalostí relevantných pre identifikáciu situácií, ktoré môžu:
 - a. viesť k tomu, že systém umelej inteligencie bude predstavovať riziko pre zdravie alebo bezpečnosť, alebo pre ochranu základných práv osôb, alebo
 - b. viesť k podstatnej zmene.
- 5.3. **<Nepovinné>** Dodávateľ umožní verejnej organizácii mať prístup k logom, ktoré sú automaticky generované systémom umelej inteligencie v reálnom čase.
- 5.4. Dodávateľ uchováva logy automaticky generované systémom umelej inteligencie do takej miery, že tieto logy sú na základe dohody pod jeho kontrolou, a to počas trvania dohody. Na konci obdobia platnosti dohody bezodkladne poskytne dodávateľ tieto logy verejnej organizácii.

Article 6 Transparentnosť systému umelej inteligencie

- 6.1. Dodávateľ zaistí to, že systém umelej inteligencie bol a je koncipovaný a vyvinutý tak, aby prevádzka systému umelej inteligencie bola dostatočne transparentná na to, aby verejná organizácia mohla primerane pochopiť fungovanie systému.
- 6.2. S cieľom zaistiť primeranú transparentnosť vykoná dodávateľ pred dodaním systému umelej inteligencie prinajmenšom technické a organizačné opatrenia opísané v **prílohe E**. Tieto opatrenia by mali viesť k tomu, že verejná organizácia bude schopná pochopiť a primerane používať systém umelej inteligencie a bude rozumieť tomu, ako systém umelej inteligencie funguje a aké údaje spracúva. Vďaka tomu bude verejná organizácia schopná vysvetliť rozhodnutia prijaté systémom umelej inteligencie osobám alebo skupinám osôb, v prípade ktorých sa systém umelej inteligencie používa (alebo má používať).

Article 7 Ľudský dohľad

- 7.1. Dodávateľ zaistí to, že systém umelej inteligencie bol a je koncipovaný a vyvinutý tak, aby nad ním mohli fyzické osoby vykonávať účinný dohľad, ktorý je primeraný rizikám spojeným s týmto systémom, a to aj pomocou vhodných nástrojov rozhrania človek – stroj.
- 7.2. Dodávateľ zaistí, aby sa do systému umelej inteligencie pred dodaním začlenili primerané opatrenia a aby sa tieto opatrenia prijali na zaistenie ľudského dohľadu. Tieto opatrenia, ktoré môžu okrem iného zahŕňať školenie zamestnancov verejnej organizácie, umožnia osobám, ktorým je zverený ľudský dohľad, aby podľa okolností:
- a. si uvedomili a dostatočne pochopili relevantné kapacity a obmedzenia systému umelej inteligencie a boli schopné riadne monitorovať jeho prevádzku tak, aby bolo možné čo najskôr odhaliť a odstrániť príznaky anomálií, porúch a neočakávaného správania systému;
 - b. si boli neustále vedomé možnosti tendencie automatického spoliehania sa alebo nadmerného spoliehania sa na výstup vytvorený systémom umelej inteligencie („automatizačné skreslenie“), a to najmä v prípade, že sa systém umelej inteligencie používa na poskytovanie informácií alebo odporúčaní pre rozhodnutia, ktoré majú prijať fyzické osoby;
 - c. boli schopné správne interpretovať výstup systému umelej inteligencie, najmä s prihliadnutím na charakteristiky systému a dostupné interpretačné nástroje a metódy;
 - d. boli schopné v akejkoľvek konkrétnej situácii rozhodnúť, že sa systém umelej inteligencie nebude používať alebo sa výstup systému umelej inteligencie inak nezohľadní, potlačí alebo zvráti;
 - e. boli schopné zasiahnuť do prevádzky systému umelej inteligencie alebo ho prerušiť tlačidlom zastavenia alebo podobným postupom.
- 7.3. **<nepovinné>** S cieľom zaistiť primeraný ľudský dohľad vykoná dodávateľ pred dodaním systému umelej inteligencie prinajmenšom technické a organizačné opatrenia opísané v **prílohe F**.

Article 8 Presnosť, spoľahlivosť a kybernetická bezpečnosť

- 8.1. Dodávateľ zaistí to, že systém umelej inteligencie bol a je koncipovaný a vyvinutý podľa zásady bezpečnosti už v štádiu návrhu a bezpečnosti ako štandardu. Vzhľadom na zamýšľaný účel by mal systém umelej inteligencie dosiahnuť primeranú úroveň presnosti, spoľahlivosti, bezpečnosti a kybernetickej bezpečnosti a fungovať z uvedených hľadísk konzistentne počas celého svojho životného cyklu.
- 8.2. Úrovne presnosti a príslušné metriky na meranie presnosti systému umelej inteligencie sú opísané v **prílohe G**.
- 8.3. S cieľom zaistiť primeranú úroveň spoľahlivosti, bezpečnosti a kybernetickej bezpečnosti vykoná dodávateľ pred dodaním systému umelej inteligencie prinajmenšom technické a organizačné opatrenia opísané v **prílohe H**.

Article 9 Súlad

- 9.1. Dodávateľ musí zaistiť, aby bol systém umelej inteligencie v súlade s týmito doložkami, a to od jeho dodania až po skončenie obdobia platnosti dohody.
- 9.2. Dodávateľ musí verejnej organizácii na jej prvé požiadanie sprístupniť všetky informácie potrebné na preukázanie súladu s týmito doložkami.
- 9.3. Ak sa dodávateľ počas obdobia platnosti dohody domnieva alebo má dôvod domnievať, že systém umelej inteligencie nie je v zhode s týmito doložkami, či už v reakcii na pripomienku verejnej organizácie, alebo nie, bezodkladne prijme potrebné nápravné opatrenia s cieľom dosiahnuť zhodu systému. Dodávateľ o tom zodpovedajúcim spôsobom informuje verejnú organizáciu.

Article 10 Povinnosť vysvetliť fungovanie systému umelej inteligencie na individuálnej úrovni

- 10.1. Okrem povinností opísaných v článku 6 je dodávateľ počas obdobia platnosti dohody povinný pomôcť verejnej organizácii na prvú žiadosť verejnej organizácie vysvetliť, ako systém umelej inteligencie dospel ku konkrétnemu rozhodnutiu alebo výsledku osobám alebo skupine osôb, v prípade ktorých sa systém umelej inteligencie používa (alebo má používať). Táto pomoc bude zahŕňať minimálne jasné pomenovanie kľúčových faktorov, ktoré viedli systém umelej inteligencie ku konkrétnemu výsledku, a zmien na úrovni vstupu, ktoré sa musia vykonať, aby systém dospel k inému výsledku.
- 10.2. Povinnosť opísaná v bode 10.1 zahŕňa poskytnutie všetkých technických a ostatných informácií potrebných na vysvetlenie spôsobu, akým systém umelej inteligencie dospel ku konkrétnemu rozhodnutiu alebo výsledku, verejnej organizácii a ponúknutie možnosti osobám alebo skupinám osôb, v prípade ktorých sa systém umelej inteligencie používa (alebo má používať), overiť spôsob, akým systém umelej inteligencie dospel ku konkrétnemu rozhodnutiu alebo výsledku. Dodávateľ týmto udeľuje verejnej organizácii právo používať, zdieľať a zverejňovať tieto informácie, ak je to potrebné na informovanie osôb alebo skupín osôb, v prípade ktorých sa systém umelej inteligencie používa (alebo má používať), o fungovaní systému umelej inteligencie a/alebo v akomkoľvek súdnom konaní, a to v potrebnom rozsahu.
- 10.3. **<nepovinné>** Povinnosti uvedené v bodoch 10.1 a 10.2 zahŕňajú zdrojový kód systému umelej inteligencie, technické špecifikácie použité pri vývoji systému umelej inteligencie, súbory údajov, technické informácie o spôsobe, akým boli súbory údajov použité pri vývoji systému umelej inteligencie získané a upravené, informácie o použitej metóde vývoja a realizovanom procese vývoja, odôvodnenie výberu konkrétneho modelu a jeho parametrov a informácie o výkonnosti systému umelej inteligencie.

Oddiel C – Práva na používanie súborov údajov

Article 11 Práva na súbory údajov verejnej organizácie

- 11.1. Všetky práva vrátane akéhokoľvek práva duševného vlastníctva, ktoré sa týkajú súborov údajov verejnej organizácie, prípadnú verejnej organizácii alebo tretej strane, ktorú verejná organizácia určí.

- 11.2. Pokiaľ nie je v prílohe B uvedené inak, dodávateľ nie je oprávnený používať súbory údajov verejnej organizácie na žiadne iné účely, ako je plnenie dohody.
- 11.3. Pokiaľ nie je v prílohe B uvedené inak, dodávateľ musí na prvé požiadanie verejnej organizácie zničiť súbory údajov verejnej organizácie. Ak si to verejná organizácia vyžiada, dodávateľ musí poskytnúť reálny dôkaz o zničení súborov údajov verejnej organizácie.

Article 12 Práva na súbory údajov dodávateľa a súbory údajov tretej strany

- 12.1. Všetky práva vrátane akéhokoľvek práva duševného vlastníctva, ktoré sa týkajú súborov údajov dodávateľa a súborov údajov tretej strany, prípadnú dodávateľovi alebo tretej strane.
- 12.2. Pokiaľ nie je v prílohe B uvedené inak, dodávateľ udeľuje verejnej organizácii nevýhradné právo používať súbory údajov dodávateľa a súbory údajov tretej strany, ktoré je v každom prípade dostatočné na plnenie ustanovení dohody vrátane doložiek.
- 12.3. **<nepovinné>** Právo na používanie opísané v bode 12.2 zahŕňa právo používať súbory údajov dodávateľa a súbory údajov tretej strany na ďalší vývoj systému umelej inteligencie vrátane všetkých jeho nových verzií, a to verejnou organizáciou alebo treťou stranou.

Article 13 Odovzdanie súborov údajov

- 13.1. Dodávateľ odovzdá verejnej organizácii na jej prvé požiadanie najnovšiu verziu súborov údajov verejnej organizácie.
- 13.2. Pokiaľ nie je v prílohe B uvedené inak, dodávateľ odovzdá verejnej organizácii na jej prvé požiadanie najnovšiu verziu súborov údajov dodávateľa a súborov údajov tretej strany.
- 13.3. Dodávateľ musí verejnej organizácii odovzdať súbory údajov v bežnom formáte súboru, ktorý určí verejná organizácia. **<nepovinné> Súbory údajov sa vrátia takto: [formát súboru]**

Príloha A – Systém umelej inteligencie a zamýšľaný účel

Popis systému umelej inteligencie

Do rozsahu pôsobnosti týchto doložiek patria tieto systémy alebo komponenty systémov:

Uvedte opis systému (systémov) umelej inteligencie. Môže ísť aj o algoritmický systém, ktorý nespĺňa požiadavky systému umelej inteligencie podľa aktu o umelej inteligencii.

Zamýšľaný účel

Uvedte opis použitia, na ktorý je systém umelej inteligencie určený.

Príloha B – Súbory údajov

Uvedte opis súborov údajov použitých na tréovanie (v prípade potreby), validáciu a testovanie systému umelej inteligencie. Rozlišujte medzi súbormi údajov verejnej organizácie, súbormi údajov dodávateľa a súbormi údajov tretej strany. V prípade súborov údajov verejnej organizácie opíšte účely, na ktoré môže dodávateľ súbory údajov použiť (iné ako plnenie dohody), a či je dodávateľ povinný na konci obdobia platnosti dohody súbory údajov zničiť. V prípade súborov údajov dodávateľa a súborov údajov tretej strany opíšte účely, na ktoré môže verejná organizácia súbory údajov použiť, a či je dodávateľ povinný súbory údajov odovzdať.

Súbory údajov verejnej organizácie

Podľa dohody poskytuje verejná organizácia dodávateľovi tieto súbory údajov, prípadne sa ako súčasť dohody majú vytvoriť alebo zhromaždiť tieto súbory údajov:

| Opis súboru údajov | Práva dodávateľa na používanie | Povinnosť zničiť súbor údajov na konci obdobia platnosti dohody |
|--------------------|--------------------------------|---|
| | | Áno/Nie |
| | | Áno/Nie |
| | | Áno/Nie |
| | | Áno/Nie |

Súbory údajov dodávateľa a súbory údajov tretej strany

Na tréovanie (v prípade potreby), validáciu a testovanie systému umelej inteligencie sa použijú alebo boli použité tieto súbory údajov dodávateľa a súbory údajov tretej strany:

| Opis súboru údajov | Práva verejnej organizácie na používanie | Povinnosť odovzdať ¹ |
|--------------------|--|---------------------------------|
| | | Áno/Nie |
| | | Áno/Nie |
| | | Áno/Nie |
| | | Áno/Nie |

¹ Obmedzenie povinnosti odovzdať súbory údajov dodávateľa a súbory údajov tretej strany neobmedzuje povinnosti dodávateľa opísané v článkoch 6 a 10.

Príloha C Technická dokumentácia

Technická dokumentácia obsahuje v závislosti od príslušného systému umelej inteligencie aspoň tieto informácie:

1. všeobecný opis systému umelej inteligencie vrátane týchto prvkov:
 - 1.1. jeho zamýšľaný účel, meno dodávateľa, dátum a verzia systému;
 - 1.2. povaha údajov, ktoré by mohli byť alebo majú byť spracované systémom, a v prípade osobných údajov kategórie fyzických osôb a skupín, ktoré by mohli byť alebo majú byť dotknuté;
 - 1.3. spôsob, akým môže systém umelej inteligencie komunikovať s hardvérom alebo softvérom, ktorý nie je súčasťou samotného systému umelej inteligencie, alebo ako ho prípadne možno na takúto interakciu použiť;
 - 1.4. verzie príslušného softvéru alebo firmvéru a všetkých požiadaviek súvisiacich s aktualizáciou verzií;
 - 1.5. opis všetkých foriem, v ktorých sa systém umelej inteligencie uvádza na trh alebo do prevádzky;
 - 1.6. opis hardvéru, na ktorom má systém umelej inteligencie fungovať;
 - 1.7. ak je systém umelej inteligencie komponentom výrobkov, fotografií alebo ilustrácií zobrazujúcich vonkajšie vlastnosti, tak označenie a vnútorné usporiadanie týchto výrobkov;
 - 1.8. podrobný a ľahko zrozumiteľný opis hlavného cieľa alebo cieľov systému v oblasti optimalizácie;
 - 1.9. podrobný a ľahko zrozumiteľný opis očakávaného výstupu systému a jeho očakávanej kvality;
 - 1.10. podrobný a ľahko zrozumiteľný návod, ako výstup systému interpretovať;
 - 1.11. príklady scenárov, v ktorých by sa systém nemal používať;

2. podrobný opis prvkov systému umelej inteligencie a procesu jeho vývoja, a to:
 - 2.1. metódy a kroky vykonané pri vývoji systému umelej inteligencie vrátane prípadného využívania vopred natrénovaných systémov alebo nástrojov poskytnutých tretími stranami a spôsobu, akým ich dodávateľ používal, integroval alebo upravil, vrátane opisu všetkých dojednaní v oblasti udeľovania licencií alebo iných zmluvných dojednaní týkajúcich sa takýchto vstupov tretích strán;
 - 2.2. špecifikácie koncepcie systému, konkrétne všeobecná logika systému umelej inteligencie a algoritmov; kľúčové rozhodnutia o koncepčných riešeniach vrátane odôvodnenia a predpokladov, a to aj so zreteľom na osoby alebo skupiny osôb, v prípade ktorých sa má systém používať; hlavné možnosti klasifikácie; čo má systém optimalizovať, a relevantnosť jednotlivých parametrov; rozhodnutia o akomkoľvek možnom kompromise vykonanom v súvislosti s technickými riešeniami prijatými na dosiahnutie súladu s požiadavkami stanovenými v týchto doložkách;
 - 2.3. opis architektúry systému, v ktorom sa vysvetľuje, ako softvérové komponenty na seba nadväzujú alebo ako sa navzájom dopĺňajú a integrujú do celkového

- spracovania; výpočtové zdroje používané na vývoj, tréning, testovanie a validáciu systému umelej inteligencie;
- 2.4. v príslušnom prípade požiadavky na údaje, pokiaľ ide o údajové hárky s opisom tréningových metodík a techník a použitých súborov tréningových údajov vrátane informácií o pôvode týchto súborov údajov, ich rozsahu a hlavných vlastnostiach; spôsob získavania a výberu údajov; postupy označovania (napr. pre učenie s učiteľom), metodiky čistenia údajov (napr. zisťovanie odľahlých hodnôt);
 - 2.5. v náležitom prípade podrobný opis vopred určených zmien systému umelej inteligencie a jeho výkonnosti spolu so všetkými relevantnými informáciami týkajúcimi sa technických riešení prijatých na zabezpečenie trvalého súladu systému umelej inteligencie s príslušnými požiadavkami stanovenými v týchto doložkách;
 - 2.6. použité postupy validácie a testovania vrátane informácií o použitých validačných a testovacích údajoch a ich hlavných vlastnostiach; metriky používané na meranie presnosti, spoľahlivosti, kybernetickej bezpečnosti a dosiahnutie súladu s inými relevantnými požiadavkami stanovenými v týchto doložkách, ako aj potenciálne diskriminačné vplyvy; testovacie logy a všetky správy o testoch s dátumom a podpisom zodpovedných osôb, a to aj pokiaľ ide o vopred určené zmeny uvedené v bode 2.5;
 - 2.7. zavedené opatrenia v oblasti kybernetickej bezpečnosti.

Podrobné informácie o monitorovaní, fungovaní a kontrole systému umelej inteligencie, najmä pokiaľ ide o: jeho schopnosti a obmedzenia výkonnosti vrátane miery presnosti v prípade konkrétnych osôb alebo skupín osôb, u ktorých sa má systém používať, a celkovú očakávanú úroveň presnosti vo vzťahu k zamýšľanému účelu; predvídateľné nezamýšľané výsledky a zdroje rizík pre zdravie a bezpečnosť, základné práva a diskrimináciu vzhľadom na zamýšľaný účel systému umelej inteligencie;

3. podrobný opis systému riadenia rizík v súlade s článkom 2;
4. opis každej relevantnej zmeny vykonanej dodávateľom v systéme počas jeho životného cyklu.

Príloha D Návod na použitie

Návod na použitie obsahuje v závislosti od systému umelej inteligencie aspoň tieto informácie:

1. totožnosť a kontaktné údaje dodávateľa a v príslušných prípadoch jeho splnomocnených zástupcov;
2. charakteristiky, schopnosti a obmedzenia výkonnosti systému umelej inteligencie a prípadne vrátane:
 - 2.1. jeho zamýšľaného účelu;
 - 2.2. úrovne presnosti, spoľahlivosti a kybernetickej bezpečnosti podľa článku 8, na základe ktorej bol systém umelej inteligencie testovaný a validovaný a ktorú možno očakávať, ako aj všetky dobre známe a predvídateľné okolnosti, ktoré môžu mať vplyv na túto očakávanú úroveň presnosti, spoľahlivosti a kybernetickej bezpečnosti;
 - 2.3. všetkých dobre známych alebo predvídateľných okolností súvisiacich s používaním systému umelej inteligencie v súlade so zamýšľaným účelom alebo za podmienok logicky predvídateľného nesprávneho použitia, ktoré môžu viesť k rizikám pre zdravie a bezpečnosť alebo pre základné práva;
 - 2.4. miera, do akej môže systém umelej inteligencie vysvetliť prijímané rozhodnutia;
 - 2.5. jeho výkonnosti, pokiaľ ide o osoby alebo skupiny osôb, v prípade ktorých sa má systém používať;
 - 2.6. relevantných informácií o činnostiach používateľov, ktoré môžu ovplyvniť výkonnosť systému, vrátane typu alebo kvality vstupných údajov alebo akýchkoľvek iných relevantných informácií z hľadiska použitých súborov tréningových, validačných a testovacích údajov, pričom sa zohľadní zamýšľaný účel systému umelej inteligencie;
3. prípadné zmeny systému umelej inteligencie a jeho výkonnosti, ktoré vopred určil dodávateľ;
4. opatrenia na zabezpečenie ľudského dohľadu uvedené v článku 7 vrátane technických opatrení zavedených na uľahčenie výkladu výstupov systému umelej inteligencie verejnou organizáciou;
5. očakávaná životnosť systému umelej inteligencie a všetky potrebné opatrenia na údržbu a starostlivosť, ktorými sa má zabezpečiť riadne fungovanie tohto systému umelej inteligencie, a to aj pokiaľ ide o aktualizácie softvéru;
6. opis mechanizmov začlenených do systému umelej inteligencie, ktorý umožňuje používateľom riadne zbierať, ukladať a interpretovať logy.

Príloha E Opatrenia na zaistenie transparentnosti

Na tomto mieste uveďte opis technických a organizačných opatrení, ktoré má dodávateľ prijať na zaistenie transparentnosti v súlade s článkom 6 doložiek.

Príloha F Opatrenia na zaistenie ľudského dohľadu

Na tomto mieste uveďte opis technických a organizačných opatrení, ktoré má dodávateľ prijať na zaistenie ľudského dohľadu v súlade s článkom 7 doložiek.

Príloha G Úrovne presnosti

Na tomto mieste opíšte požadované úrovne presnosti.

Príloha H Opatrenia na zaistenie primeranej úrovne spoľahlivosti, bezpečnosti a kybernetickej bezpečnosti

Na tomto mieste uveďte opis technických a organizačných opatrení, ktoré má dodávateľ prijať na zaistenie primeranej úrovne spoľahlivosti, bezpečnosti a kybernetickej bezpečnosti v súlade s článkom 8 doložiek.

Týmito opatreniami sa musí zaistiť, aby systém umelej inteligencie bol čo najodolnejší voči chybám, poruchám alebo nezrovnalostiam, ktoré sa môžu vyskytnúť v rámci systému alebo prostredia, v ktorom sa systém prevádzkuje, a to najmä z dôvodu ich interakcie s fyzickými osobami alebo inými systémami.

Systém umelej inteligencie musí byť odolný voči pokusom neoprávnených tretích strán o zmenu ich používania, správania, výstupov alebo výkonnosti využívaním zraniteľností systému. Technické riešenia na riešenie zraniteľností špecifických pre umelú inteligenciu môžu v prípade potreby zahŕňať opatrenia na prevenciu, odhaľovanie, riešenie a kontrolu útokov, ktoré sa pokúšajú manipulovať súbor tréningových údajov („otrávenie údajov“), alebo vopred tréningových komponentov používaných pri tréningu („modelové otrávenie“), vstupov upravených tak, aby model urobil chybu („odporujúce si príklady“ alebo „modelový únik“), útokov na dôvernosť alebo nedostatkov modelu, ktoré by mohli viesť k škodlivým rozhodnutiam, ako aj opatrenia s cieľom reagovať na ne.