



Procurement of AI Community

● PUBLIC BUYERS COMMUNITY

Propozycja standardowych klauzul umownych dotyczących zamówień na sztuczną inteligencję dokonywanych przez organizacje publiczne – wersja z września 2023 r. - wersja uproszczona

DRAFT– Non High Risk version

Zastrzeżenie prawne

Jest to projekt dokumentu przeznaczony wyłącznie do dyskusji służącej zebraniu wstępnych informacji zwrotnych od zainteresowanych stron. Niniejszy dokument opracował Jeroen Naves (Pels Rijcken). Nie jest to urzędowy dokument UE i w żadnym razie nie można go traktować jako wyraz oficjalnego stanowiska Komisji Europejskiej. Ani Komisja Europejska, ani żadna osoba działająca w imieniu Komisji nie ponosi odpowiedzialności za sposób wykorzystania niniejszego dokumentu. Prace nad niniejszym dokumentem są nadal w toku. Z niniejszego dokumentu nie wynikają żadne prawa.

Uwagi wstępne

Niniejszy projekt standardowych klauzul umownych przygotowano z myślą o organizacjach publicznych, które chcą dokonać zamówienia na system sztucznej inteligencji opracowany przez zewnętrznego dostawcę. Sporządzono go w oparciu o standardowe klauzule dotyczące zamówień na systemy algorytmiczne opracowane w 2018 r. przez Miasto Amsterdam (<https://www.amsterdam.nl/innovatie/digitalisering-technologie/algoritmen-ai/contractual-terms-for-algorithms/>).

Przedstawione standardowe klauzule umowne opierają się w dużej mierze na wymogach i obowiązkach dotyczących systemów sztucznej inteligencji wysokiego ryzyka, o których mowa w tytule III wniosku dotyczącego rozporządzenia w sprawie sztucznej inteligencji* („akt w sprawie sztucznej inteligencji”). Wniosek ten jest przedmiotem trwających negocjacji, dlatego klauzule będą musiały zostać zmienione, aby uwzględnić w nich wszelkie dokonane zmiany i w pełni dostosować je do ostatecznej wersji rozporządzenia przyjętego przez Radę i Parlament Europejski.

Ponieważ negocjacje w sprawie proponowanego aktu w sprawie sztucznej inteligencji są nadal w toku, organizacje publiczne, które zdecydują się na skorzystanie ze standardowych klauzul umownych, mogą to uczynić na zasadzie dobrowolności, oceniając w indywidualnych przypadkach, czy poszczególne sekcje niniejszych standardowych klauzul umownych są wystarczające i proporcjonalne na potrzeby zamówienia konkretnego systemu sztucznej inteligencji. Pełna wersja standardowych klauzul umownych dotyczy w szczególności systemów sztucznej inteligencji sklasyfikowanych jako systemy „wysokiego ryzyka” w rozumieniu art. 6 i wymienionych w jednym z obszarów objętych zakresem załączników II i III proponowanego aktu w sprawie sztucznej inteligencji.

W przepisach aktu w sprawie sztucznej inteligencji nie przewidziano obowiązku stosowania tych wymagań w odniesieniu do systemów sztucznej inteligencji niesklasyfikowanych jako systemy wysokiego ryzyka. Jest to jednak zalecane w celu zwiększenia wiarygodności aplikacji opartych na sztucznej inteligencji zamawianych przez organizacje publiczne. Niniejsza uproszczona wersja standardowych klauzul umownych dotyczy w szczególności systemów sztucznej inteligencji innych niż systemy sztucznej inteligencji wysokiego ryzyka.

W stosownych przypadkach uzasadnionych oddziaływaniem danego systemu na osoby prywatne i społeczeństwo organizacje publiczne mogą również rozszerzyć zakres stosowania niniejszych klauzul (w wersji pełnej lub uproszczonej) na inne systemy algorytmiczne, które niekoniecznie muszą być sklasyfikowane jako „sztuczna inteligencja”, aby objąć nim dodatkowo prostsze systemy oprogramowania oparte na regułach, biorąc pod uwagę, że ich wykorzystanie w sektorze publicznym może w niektórych przypadkach wymagać również zwiększonej odpowiedzialności, kontroli i przejrzystości.

Standardowe klauzule umowne zawierają wyłącznie postanowienia dotyczące systemów sztucznej inteligencji i kwestii objętych zakresem proponowanego aktu w sprawie sztucznej inteligencji. Oznacza to, że wyłączono z nich inne obowiązki lub wymagania, które mogą wynikać z odpowiednich mających zastosowanie przepisów, takich jak ogólne

rozporządzenie o ochronie danych. Ponadto niniejsze standardowe klauzule umowne nie obejmują pełnych ustaleń umownych. Na przykład nie zawierają one żadnych warunków dotyczących własności intelektualnej, akceptacji, płatności, terminów dostawy, prawa mającego zastosowanie lub odpowiedzialności. Standardowe klauzule umowne opracowano w taki sposób, aby mogły one stanowić aneks do umowy, która zawiera już ustalenia dotyczące tych kwestii.

* Wniosek dotyczący rozporządzenia Parlamentu Europejskiego i Rady ustanawiającego zharmonizowane przepisy dotyczące sztucznej inteligencji i zmieniającego niektóre akty ustawodawcze Unii, COM(2021) 206 final.

Sekcja A – Definicje

Article 1 Definicje

1.1. Następujące pojęcia używane w niniejszych klauzulach mają znaczenie zdefiniowane w niniejszym artykule:

- umowa: cała umowa, której integralną częścią są klauzule stanowiące aneks;
- system sztucznej inteligencji: system lub systemy sztucznej inteligencji wymienione w **załączniku A**, w tym wszelkie ich nowe wersje;
- klauzule: niniejsze standardowe klauzule umowne dotyczące zamówień na sztuczną inteligencję dokonywanych przez organizacje publiczne;
- zbiory danych organizacji publicznej: zbiory danych (lub ich części), które (i) zostały przekazane dostawcy przez organizację publiczną na podstawie umowy lub (ii) które mają zostać utworzone lub zebrane w ramach umowy, w tym wszelkie zmodyfikowane lub rozszerzone wersje zbiorów danych wymienionych w pkt (i) i (ii) (na przykład w związku z anotacją, etykietowaniem, czyszczeniem, wzbogaceniem lub agregacją danych);
- zbiory danych: wszystkie zbiory danych wykorzystywane do opracowania systemu sztucznej inteligencji, w tym zbiór lub zbiory danych opisane w **załączniku B**;
- dostarczenie: chwila, w której dostawca informuje organizację publiczną, że system sztucznej inteligencji spełnia wszystkie uzgodnione warunki i jest gotowy do użytku;
- przeznaczenie: zastosowanie, do jakiego system sztucznej inteligencji został przeznaczony przez organizację publiczną, w tym szczególny kontekst i warunki wykorzystywania, jak określono w załączniku B, informacjach dostarczonych przez dostawcę zawartych w instrukcji obsługi, materiałach promocyjnych lub sprzedażowych i oświadczeniach, jak również w dokumentacji technicznej;
- dające się racjonalnie przewidzieć niewłaściwe wykorzystanie: wykorzystanie systemu sztucznej inteligencji w sposób niezgodny z jego przeznaczeniem, które może wynikać z dającego się racjonalnie przewidzieć zachowania człowieka lub interakcji z innymi systemami;
- istotna zmiana: zmiana w systemie sztucznej inteligencji po jego dostarczeniu, która wpływa na zgodność tego systemu z wymogami określonymi w niniejszych klauzulach lub powoduje zmianę przeznaczenia;
- dostawca: osoba fizyczna lub prawna, organ publiczny, agencja lub inny podmiot, które dostarczają system sztucznej inteligencji organizacji publicznej zgodnie z umową;
- zbiory danych dostawcy i zbiory danych osób trzecich: zbiory danych (lub ich części), które nie kwalifikują się jako zbiory danych organizacji publicznej.

Sekcja B – Podstawowe wymagania w odniesieniu do systemu sztucznej inteligencji

Article 2 System zarządzania ryzykiem

2.1. Przed dostarczeniem systemu sztucznej inteligencji dostawca zapewnia ustanowienie i wdrożenie w odniesieniu do przedmiotowego systemu sztucznej inteligencji systemu zarządzania ryzykiem.

- 2.2. System zarządzania ryzykiem musi obejmować co najmniej następujące etapy:
 - a. identyfikację, oszacowanie i ocenę znanego i dającego się przewidzieć ryzyka dla zdrowia, bezpieczeństwa i praw podstawowych Unii Europejskiej, które może wystąpić w świetle przeznaczenia systemu sztucznej inteligencji i dającego się racjonalnie przewidzieć niewłaściwego wykorzystania;
 - b. ocenę innego mogącego wystąpić ryzyka;
 - c. przyjęcie odpowiednich i ukierunkowanych środków zarządzania ryzykiem służących wyeliminowaniu ryzyka zidentyfikowanego zgodnie z lit. a) i b) niniejszego ustępu zgodnie z przepisami dalszych ustępów.
- 2.3. Środki zarządzania ryzykiem, o których mowa w art. 2 ust. 2 lit. c), muszą być takie, aby istotne ryzyko szczątkowe związane z każdym zagrożeniem, jak również ogólne ryzyko szczątkowe systemu sztucznej inteligencji było – według racjonalnej oceny – akceptowalne dla dostawcy, pod warunkiem że system sztucznej inteligencji wykorzystuje się zgodnie z jego przeznaczeniem lub w warunkach dającego się racjonalnie przewidzieć niewłaściwego wykorzystania.
- 2.4. Przy określaniu najodpowiedniejszych środków zarządzania ryzykiem, o których mowa w ust. 2.2 lit. c), należy zapewnić:
 - a. eliminację lub ograniczenie zidentyfikowanego ryzyka w zakresie, w jakim jest to technicznie możliwe, poprzez odpowiedni projekt i odpowiednie opracowanie systemu sztucznej inteligencji;
 - b. w stosownych przypadkach wdrożenie odpowiednich środków służących ograniczeniu i kontroli ryzyka, którego nie można wyeliminować;
 - c. przekazywanie odpowiednich informacji organizacji publicznej.
- 2.5. Przed dostarczeniem systemu sztucznej inteligencji dostawca zapewnia poddanie go testom w celu sprawdzenia, czy system ten jest zgodny z postanowieniami klauzul oraz czy środki zarządzania ryzykiem, o których mowa w art. 2 ust. 2 lit. c), są skuteczne w świetle przeznaczenia i dającego się racjonalnie przewidzieć niewłaściwego wykorzystania. Na żądanie organizacji publicznej dostawca ma obowiązek przeprowadzenia testów systemu sztucznej inteligencji w środowisku organizacji publicznej.
- 2.6. Dostawca musi udokumentować wszystkie zidentyfikowane rodzaje ryzyka, wprowadzone środki i testy przeprowadzone w kontekście zgodności z niniejszym artykułem. Dostawca musi udostępnić tę dokumentację organizacji publicznej najpóźniej w chwili dostarczenia systemu sztucznej inteligencji. Dokumentacja ta może być częścią dokumentacji technicznej lub instrukcji obsługi.
- 2.7. System zarządzania ryzykiem składa się z ciągłego i iteracyjnego procesu realizowanego przez cały czas obowiązywania umowy. Po dostarczeniu systemu sztucznej inteligencji dostawca musi zatem:
 - a. dokonywać regularnego przeglądu i aktualizacji procesu zarządzania ryzykiem, aby zapewnić jego stałą skuteczność;
 - b. aktualizować dokumentację opisaną w art. 2 ust. 6 oraz
 - c. niezwłocznie udostępnić organizacji publicznej każdą nową wersję dokumentacji opisanej w art. 2 ust. 6.
- 2.8. Jeżeli dostawca zasadnie wymaga tego na potrzeby prawidłowej realizacji systemu zarządzania ryzykiem, organizacja publiczna przekaze informacje na żądanie dostawcy, o ile nie są one poufne.

- 2.9. **<opcjonalnie>** Jeżeli organizacja publiczna wykorzystuje system sztucznej inteligencji dłużej niż okres obowiązywania umowy, wówczas po upływie okresu obowiązywania umowy dostawca przekazuje jej informacje niezbędne do samodzielnego utrzymania systemu zarządzania ryzykiem.

Article 3 **< Art. 3 jest istotny wyłącznie w przypadku systemów sztucznej inteligencji, które wykorzystują techniki obejmujące trenowanie modeli z wykorzystaniem danych. Art. 3 zakłada pełny dostęp dostawcy (lub jego podwykonawców) do zbiorów danych. Jeżeli zbiory danych znajdują się wyłącznie w posiadaniu organizacji publicznej, konieczne jest dokonanie innych ustaleń.>** Dane i zarządzanie danymi

- 3.1. Dostawca zapewnia, aby zbiory danych wykorzystywane do opracowywania systemu sztucznej inteligencji, w tym zbiory danych treningowych, walidacyjnych i testowych, były objęte zarządzaniem danymi odpowiednim do kontekstu wykorzystania, a także przeznaczenia przedmiotowego systemu sztucznej inteligencji. Środki te dotyczą w szczególności:
- a. przejrzystości w odniesieniu do pierwotnego celu gromadzenia danych;
 - b. odpowiednich decyzji projektowych;
 - c. procesów gromadzenia danych;
 - d. operacji przetwarzania na potrzeby przygotowania danych, takich jak anotowanie, etykietowanie, czyszczenie, wzbogacanie i agregacja danych;
 - e. sformułowania odpowiednich założeń, zwłaszcza w odniesieniu do informacji, do których pomiaru i reprezentowania mają służyć dane;
 - f. badania pod kątem ewentualnej tendencyjności, która może mieć wpływ na zdrowie i bezpieczeństwo osób fizycznych lub prowadzić do dyskryminacji zakazanej przez przepisy Unii Europejskiej;
 - g. odpowiednich środków służących zapobieganiu, wykrywaniu i łagodzeniu ewentualnej tendencyjności;
 - h. określenia istotnych luk w danych lub braków w danych, które uniemożliwiają zapewnienie zgodności z niniejszymi klauzulami, oraz tego, w jaki sposób można zaradzić tym lukom i brakom.
- 3.2. Dostawca zapewnia, aby zbiory danych wykorzystywane przy opracowywaniu systemu sztucznej inteligencji były adekwatne, reprezentatywne, w jak największym stopniu wolne od błędów i jak najbardziej kompletne z punktu widzenia przeznaczenia. Dostawca zapewnia, aby zbiory danych charakteryzowały się odpowiednimi właściwościami statystycznymi, w tym, w stosownych przypadkach, w odniesieniu do osób lub grup osób, względem których system sztucznej inteligencji ma być wykorzystywany. Zbiory danych muszą spełniać wymienione kryteria na poziomie pojedynczych zbiorów danych lub ich kombinacji.
- 3.3. Dostawca zapewnia, aby zbiory danych wykorzystywane przy opracowywaniu systemu sztucznej inteligencji uwzględniały – w zakresie wymaganym z uwagi na ich przeznaczenie lub dające się racjonalnie przewidzieć niewłaściwe wykorzystanie – cechy lub elementy, które są specyficzne dla określonego kontekstu geograficznego, behawioralnego lub

funkcjonalnego lub okoliczności, w których system sztucznej inteligencji ma być wykorzystywany.

- 3.4. Obowiązki wynikające z niniejszego artykułu mają zastosowanie nie tylko do procesu opracowywania systemu sztucznej inteligencji przed jego dostarczeniem, ale również do każdego wykorzystania zbiorów danych przez dostawcę, które może mieć wpływ na funkcjonowanie systemu sztucznej inteligencji w dowolnym innym momencie w okresie obowiązywania umowy.

Article 4 Dokumentacja techniczna i instrukcja obsługi

- 4.1. Dostarczenie systemu sztucznej inteligencji przez dostawcę obejmuje przekazanie dokumentacji technicznej i instrukcji obsługi.
- 4.2. Dokumentacja techniczna musi umożliwiać organizacji publicznej lub osobie trzeciej ocenę zgodności systemu sztucznej inteligencji z wymogami określonymi w niniejszych klauzulach oraz spełnienie co najmniej warunków opisanych w **załączniku C**.
- 4.3. Instrukcja obsługi musi zawierać zwięzłe, kompletne, poprawne i jasne informacje, które są istotne, dostępne i zrozumiałe dla organizacji publicznej. Instrukcja obsługi musi spełniać przynajmniej warunki opisane w **załączniku D**.
- 4.4. Dostawca musi aktualizować tę dokumentację co najmniej przy każdej istotnej zmianie w okresie obowiązywania umowy, a następnie udostępnić ją organizacji publicznej.
- 4.5. **<opcjonalnie>** Dokumentację techniczną i instrukcję obsługi należy sporządzić w języku angielskim.
- 4.6. **<opcjonalnie>** Organizacja publiczna ma prawo do sporządzania kopii dokumentacji technicznej i instrukcji obsługi w zakresie niezbędnym do użytku wewnętrznego w ramach swojej struktury, bez uszczerbku dla postanowień art. 6 i 10.

Article 5 Rejestrowanie zdarzeń

- 5.1. Dostawca zapewnia, aby system sztucznej inteligencji projektowano i opracowywano w taki sposób, aby zawierał on funkcję umożliwiającą automatyczne rejestrowanie zdarzeń („rejstry zdarzeń”) podczas działania systemu. Ta funkcja rejestracji zdarzeń musi być zgodna z aktualnym stanem wiedzy oraz uznanymi normami lub wspólnymi specyfikacjami, jeżeli są dostępne. **<opcjonalnie: należy dodać konkretną normę, jeżeli jest dostępna>**
- 5.2. Funkcja rejestracji zdarzeń musi zapewnić, w całym cyklu życia systemu sztucznej inteligencji, poziom identyfikowalności jego funkcjonowania odpowiedni do przeznaczenia systemu oraz dającego się racjonalnie przewidzieć niewłaściwego wykorzystania. W szczególności funkcja ta musi umożliwiać rejestrację wszystkich zdarzeń istotnych z punktu widzenia identyfikacji sytuacji, które mogą:
- powodować, że system sztucznej inteligencji będzie stwarzać zagrożenie dla zdrowia, bezpieczeństwa lub ochrony praw podstawowych obywateli lub
 - prowadzić do istotnej zmiany.
- 5.3. **<opcjonalnie>** Dostawca zapewni organizacji publicznej dostęp do rejestrów zdarzeń generowanych automatycznie przez system sztucznej inteligencji w czasie rzeczywistym.

- 5.4. Dostawca musi przechowywać rejestry zdarzeń generowane automatycznie przez system sztucznej inteligencji w zakresie, w jakim tego rodzaju rejestry zdarzeń znajdują się pod jego kontrolą zgodnie z postanowieniami umowy i przez cały okres jej obowiązywania. Po zakończeniu okresu obowiązywania umowy dostawca niezwłocznie przekaze te rejestry organizacji publicznej.

Article 6 Przejrzystość systemu sztucznej inteligencji

- 6.1. Dostawca zapewnia, aby system sztucznej inteligencji projektowano i opracowywano w taki sposób, aby jego działanie było wystarczająco przejrzyste i umożliwiało organizacji publicznej odpowiednie zrozumienie jego funkcjonowania.
- 6.2. Aby zapewnić odpowiednią przejrzystość, przed dostarczeniem systemu sztucznej inteligencji dostawca musi wdrożyć przynajmniej środki techniczne i organizacyjne opisane w **załączniku E**. Środki te powinny umożliwić odpowiednie zrozumienie i stosowanie system sztucznej inteligencji przez organizację publiczną, która, dzięki zrozumieniu sposobu jego działania i rodzajów przetwarzanych danych, będzie w stanie wyjaśnić decyzje podejmowane przez system sztucznej inteligencji osobom lub grupom osób, względem których system ten jest (ma być) wykorzystywany.

Article 7 Sprawowanie nadzoru przez człowieka

- 7.1. Dostawca zapewnia, aby system sztucznej inteligencji projektowano i opracowywano w taki sposób, w tym poprzez uwzględnienie odpowiednich narzędzi interfejsu człowiek-maszyna, aby osoby fizyczne mogły sprawować nad nim skuteczny nadzór, współmiernie do związanego z tym systemem ryzyka.
- 7.2. Dostawca zapewnia, aby przed dostarczeniem systemu sztucznej inteligencji wbudowano w niego i wprowadzono odpowiednie środki zapewniające sprawowanie nadzoru przez człowieka. Środki te – które mogą obejmować między innymi szkolenie pracowników organizacji publicznej – muszą umożliwiać osobom, którym powierzono sprawowanie nadzoru, odpowiednio do okoliczności:
- a. świadomość i zrozumienie w wystarczającym stopniu odpowiednich możliwości i ograniczeń systemu sztucznej inteligencji oraz należyte monitorowanie jego działania, tak aby oznaki anomalii, nieprawidłowego funkcjonowania i nieoczekiwanych wyników działania można było wykrywać i zaradzić im tak szybko, jak to możliwe;
 - b. bycie stale świadomym potencjalnej tendencji do automatycznego polegania lub nadmiernego polegania na wyniku działania systemu sztucznej inteligencji (tzw. „automation bias”), w szczególności w przypadku gdy system sztucznej inteligencji jest wykorzystywany do udzielania informacji lub zaleceń na potrzeby decyzji podejmowanych przez osoby fizyczne;
 - c. prawidłową interpretację wyniku działania systemu sztucznej inteligencji, biorąc pod uwagę w szczególności cechy systemu oraz dostępne narzędzia i metody interpretacji;

- d. podjęcie decyzji, w każdej konkretnej sytuacji, o niekorzystaniu z systemu sztucznej inteligencji lub w inny sposób zignorowanie, ręczną zmianę lub odwrócenie wyniku działania systemu sztucznej inteligencji;
 - e. ingerowanie w działanie systemu sztucznej inteligencji lub przerwanie działania systemu za pomocą przycisku „stop” lub podobnej procedury.
- 7.3. **<opcjonalnie>** Aby zapewnić odpowiednie sprawowanie nadzoru przez człowieka, przed dostarczeniem systemu sztucznej inteligencji dostawca musi wdrożyć przynajmniej środki techniczne i organizacyjne opisane w **załączniku F**.

Article 8 Dokładność, solidność i cyberbezpieczeństwo

- 8.1. Dostawca zapewnia, aby system sztucznej inteligencji projektowano i opracowywano zgodnie z zasadą zakładającą uwzględnianie bezpieczeństwa już na etapie projektowania i jako opcji domyślnej. Z uwagi na swoje przeznaczenie system sztucznej inteligencji powinien osiągać odpowiedni poziom dokładności, solidności, bezpieczeństwa i cyberbezpieczeństwa oraz zachować pod tymi względami niezmienną skuteczność działania przez cały cykl życia.
- 8.2. Poziomy dokładności i odpowiednie wskaźniki dokładności systemu sztucznej inteligencji opisano w **załączniku G**.
- 8.3. Aby zapewnić odpowiedni poziom solidności, bezpieczeństwa i cyberbezpieczeństwa, przed dostarczeniem systemu sztucznej inteligencji dostawca musi wdrożyć przynajmniej środki techniczne i organizacyjne opisane w **załączniku H**.

Article 9 Zgodność

- 9.1. Dostawca musi zapewnić, aby od chwili dostarczenia systemu sztucznej inteligencji do końca okresu obowiązywania umowy system sztucznej inteligencji był zgodny z niniejszymi klauzulami.
- 9.2. Na pierwszy wniosek organizacji publicznej dostawca musi udostępnić jej wszystkie informacje niezbędne do wykazania zgodności z niniejszymi klauzulami.
- 9.3. Jeżeli w okresie obowiązywania umowy dostawca uzna lub będzie miał powody, aby uznać, że system sztucznej inteligencji nie jest zgodny z niniejszymi klauzulami – niezależnie od tego, czy nastąpi to w reakcji na uwagę organizacji publicznej, czy też nie – musi niezwłocznie podjąć niezbędne działania naprawcze w celu zapewnienia zgodności systemu. Dostawca musi poinformować o nich organizację publiczną.

Article 10 Obowiązek wyjaśnienia funkcjonowania systemu sztucznej inteligencji na poziomie indywidualnym

- 10.1. Poza obowiązkami opisanymi w art. 6 w okresie obowiązywania umowy dostawca jest zobowiązany do udzielenia organizacji publicznej, na jej pierwszy wniosek, pomocy w wyjaśnieniu osobom lub grupom osób, względem których system sztucznej inteligencji jest (ma być) wykorzystywany, w jaki sposób system ten podjął daną decyzję lub uzyskał dany wynik. Pomoc ta będzie obejmować co najmniej wyraźne wskazanie kluczowych

- czynników, które sprawiły, że system sztucznej inteligencji uzyskał dany wynik, oraz zmian w danych wejściowych, które należy wprowadzić, aby osiągnąć inny wynik.
- 10.2. Obowiązek opisany w art. 10 ust. 1 obejmuje przekazanie organizacji publicznej wszystkich informacji technicznych oraz innych informacji wymaganych w celu wyjaśnienia, w jaki sposób system sztucznej inteligencji podjął daną decyzję lub uzyskał dany wynik, a także w celu zapewnienia osobom lub grupie osób, względem których system sztucznej inteligencji jest (ma być) wykorzystywany, możliwość sprawdzenia sposobu, w jaki system sztucznej inteligencji podjął daną decyzję lub uzyskał dany wynik. Dostawca niniejszym przyznaje organizacji publicznej prawo do wykorzystywania, udostępniania i ujawniania tych informacji, jeżeli (i w zakresie, w jakim) jest to niezbędne, aby poinformować osoby lub grupy osób, względem których system sztucznej inteligencji jest (ma być) wykorzystywany, o funkcjonowaniu tego systemu lub w toku postępowania sądowego.
- 10.3. **<opcjonalnie>** Obowiązki, o których mowa w art. 10 ust. 1 i 2, obejmują kod źródłowy systemu sztucznej inteligencji, specyfikacje techniczne wykorzystane przy opracowywaniu systemu sztucznej inteligencji, zbiory danych, informacje techniczne na temat sposobu pozyskiwania i edycji zbiorów danych wykorzystanych do opracowania systemu sztucznej inteligencji, informacje na temat zastosowanej metody opracowywania i przeprowadzonego procesu opracowywania, uzasadnienie wyboru konkretnego modelu i jego parametrów oraz informacje na temat skuteczności działania systemu sztucznej inteligencji.

Sekcja C – Prawa do wykorzystywania zbiorów danych

Article 11 Prawa do zbiorów danych organizacji publicznej

- 11.1. Wszystkie prawa, w tym wszelkie prawa własności intelektualnej, związane ze zbiorami danych organizacji publicznej będą przysługiwać organizacji publicznej lub osobie trzeciej wyznaczonej jako taka przez organizację publiczną.
- 11.2. Dostawca nie jest uprawniony do wykorzystywania zbiorów danych organizacji publicznej do celów innych niż wykonanie umowy, chyba że załącznik B stanowi inaczej.
- 11.3. Na pierwszy wniosek organizacji publicznej dostawca musi zniszczyć zbiory danych organizacji publicznej, chyba że załącznik B stanowi inaczej. Na żądanie organizacji publicznej dostawca musi przedstawić wiarygodne dowody potwierdzające zniszczenie zbiorów danych organizacji publicznej.

Article 12 Prawa do zbiorów danych dostawcy i zbiorów danych osób trzecich

- 12.1. Wszystkie prawa, w tym wszelkie prawa własności intelektualnej, związane ze zbiorami danych dostawcy i zbiorami danych osób trzecich będą przysługiwać dostawcy lub osobie trzeciej.
- 12.2. Dostawca przyznaje organizacji publicznej niewyłączne prawo do wykorzystywania zbiorów danych dostawcy i zbiorów danych osób trzecich, które w każdym przypadku jest wystarczające do wykonania postanowień umowy, w tym klauzul, chyba że załącznik B stanowi inaczej.
- 12.3. **<opcjonalnie>** Prawo do wykorzystywania opisane w art. 12 ust. 2 obejmuje prawo do wykorzystywania zbiorów danych dostawcy i zbiorów danych osób trzecich w celu dalszego

rozwijania systemu sztucznej inteligencji, w tym wszelkich jego nowych wersji, przez organizację publiczną lub osobę trzecią.

Article 13 Przekazywanie zbiorów danych

- 13.1. Na pierwszy wniosek organizacji publicznej dostawca prześle jej najnowszą wersję zbioru danych organizacji publicznej.
- 13.2. Na pierwszy wniosek organizacji publicznej dostawca prześle jej najnowszą wersję zbiorów danych dostawcy i zbiorów danych osób trzecich, chyba że załącznik B stanowi inaczej.
- 13.3. Dostawca musi przekazać organizacji publicznej zbiory danych w powszechnie stosowanym formacie pliku, który zostanie wskazany przez organizację publiczną. **<opcjonalnie> Zbiory danych zostaną przekazane w następujący sposób: [format pliku].**

Załącznik A – System sztucznej inteligencji i jego przeznaczenie

Opis systemu sztucznej inteligencji

Zakres niniejszych klauzul obejmuje następujące systemy lub elementy systemów:

Proszę opisać system(y) sztucznej inteligencji. Może być to również system algorytmiczny, który nie kwalifikuje się jako system sztucznej inteligencji na podstawie aktu w sprawie sztucznej inteligencji.

Przeznaczenie

Proszę opisać wykorzystanie, do którego jest przeznaczony system sztucznej inteligencji.

Załącznik B – Zbiory danych

Proszę opisać zbiory danych wykorzystywane do celów trenowania (jeżeli dotyczy), walidacji i testowania systemu sztucznej inteligencji. Rozróżnienie między zbiorami danych organizacji publicznej a zbiorami danych dostawcy i zbiorami danych osób trzecich. W przypadku zbiorów danych organizacji publicznej proszę opisać cele, do jakich dostawca może wykorzystywać zbiory danych (inne niż wykonanie umowy), oraz czy dostawca ma obowiązek zniszczenia zbioru danych po zakończeniu okresu obowiązywania umowy. W przypadku zbiorów danych dostawcy i zbiorów danych osób trzecich proszę opisać cele, do jakich organizacja publiczna może wykorzystywać zbiory danych, oraz czy dostawca ma obowiązek przekazania zbiorów danych.

Zbiory danych organizacji publicznej

Na podstawie umowy następujące zbiory danych zostaną przekazane dostawcy przez organizację publiczną lub zostaną utworzone lub zebrane w ramach umowy:

Opis zbioru danych	Prawa użytkowania przysługujące dostawcy	Obowiązek zniszczenia zbioru danych po zakończeniu okresu obowiązywania umowy
		Tak/Nie
		Tak/Nie
		Tak/Nie
		Tak/Nie

Zbiory danych dostawcy i zbiory danych osób trzecich:

Następujące zbiory danych dostawcy i zbiory danych osób trzecich będą lub były wykorzystywane do celów trenowania (jeżeli dotyczy), walidacji i testowania systemu sztucznej inteligencji:

Opis zbioru danych	Prawa użytkowania przysługujące organizacji publicznej	Obowiązek przekazania ¹
		Tak/Nie
		Tak/Nie

¹ Ograniczenie obowiązku przekazania zbiorów danych dostawcy i zbiorów danych osób trzecich nie ogranicza obowiązków dostawcy opisanych w art. 6 i 10.

Załącznik C Dokumentacja techniczna

Dokumentacja techniczna powinna zawierać, stosownie do przypadku, co najmniej następujące informacje właściwe dla danego systemu sztucznej inteligencji:

1. Ogólny opis systemu sztucznej inteligencji, w tym:
 - 1.1. jego przeznaczenie, nazwę dostawcy oraz datę i wersję systemu;
 - 1.2. charakter danych, które mogą lub mają być przetwarzane przez system, oraz, w przypadku danych osobowych, kategorie osób fizycznych i grup, których dane mogą lub mają być przetwarzane;
 - 1.3. sposób, w jaki system sztucznej inteligencji, w stosownych przypadkach, może współdziałać lub może być wykorzystany do współdziałania ze sprzętem lub oprogramowaniem, które nie są częścią samego systemu sztucznej inteligencji;
 - 1.4. wersje odpowiedniego oprogramowania lub oprogramowania układowego oraz wszelkie wymagania związane z aktualizacją wersji;
 - 1.5. opis wszystkich form, w jakich system sztucznej inteligencji wprowadza się do obrotu lub oddaje do użytku;
 - 1.6. opis sprzętu, na którym system sztucznej inteligencji ma być eksploatowany;
 - 1.7. w przypadku gdy system sztucznej inteligencji jest elementem produktów – zdjęcia lub ilustracje przedstawiające cechy zewnętrzne, oznakowanie i układ wewnętrzny tych produktów;
 - 1.8. szczegółowy i zrozumiały opis głównego celu lub głównych celów w zakresie optymalizacji systemu;
 - 1.9. szczegółowy i zrozumiały opis oczekiwanych wyników działania systemu i oczekiwanej jakości wyników;
 - 1.10. szczegółowe i zrozumiałe instrukcje dotyczące interpretacji wyników działania systemu;
 - 1.11. przykłady scenariuszy, w których system nie powinien być wykorzystywany.
2. Szczegółowy opis elementów systemu sztucznej inteligencji oraz procesu jego opracowywania, w tym:
 - 2.1. metody i działania zastosowane w celu opracowania systemu sztucznej inteligencji, w tym, w stosownych przypadkach, skorzystanie z już wytrenowanych systemów lub narzędzi dostarczonych przez osoby trzecie oraz wskazanie, w jaki sposób dostawca wykorzystał, zintegrował lub zmodyfikował te systemy lub narzędzia, w tym opis wszelkich ustaleń licencyjnych i umownych dotyczących takiego wkładu osób trzecich;
 - 2.2. specyfikacje projektowe systemu, a mianowicie ogólna logika systemu sztucznej inteligencji i algorytmów; kluczowe decyzje projektowe wraz z uzasadnieniem i przyjętymi założeniami, również w odniesieniu do osób lub grup osób, względem których system ma być wykorzystywany; główne wybory klasyfikacyjne; wskazanie, pod kątem czego system ma być optymalizowany, i znaczenie poszczególnych parametrów; decyzje dotyczące wszelkich

- możliwych kompromisów w zakresie rozwiązań technicznych przyjętych w celu spełnienia wymogów określonych w niniejszych klauzulach;
- 2.3. opis architektury systemu wyjaśniający, w jaki sposób elementy oprogramowania współgrają ze sobą lub wzajemnie się uzupełniają oraz włączają się w ogólne przetwarzanie; zasoby obliczeniowe wykorzystywane do opracowania, trenowania, testowania i walidacji systemu sztucznej inteligencji;
 - 2.4. w stosownych przypadkach wymogi dotyczące danych w formie arkuszy danych opisujących metodyki i techniki trenowania systemu oraz wykorzystane zbiory danych treningowych, w tym informacje o pochodzeniu tych zbiorów danych, ich zakresie i głównych cechach; sposób, w jaki uzyskano i wybrano dane; procedury etykietowania (np. w przypadku uczenia nadzorowanego), metody oczyszczania danych (np. wykrywanie wartości oddalonych);
 - 2.5. w stosownych przypadkach szczegółowy opis z góry zaplanowanych zmian w systemie sztucznej inteligencji i jego skuteczności działania wraz ze wszystkimi istotnymi informacjami dotyczącymi rozwiązań technicznych przyjętych w celu zapewnienia ciągłej zgodności systemu sztucznej inteligencji z odpowiednimi wymogami określonymi w niniejszych klauzulach;
 - 2.6. zastosowane procedury walidacji i testowania, w tym informacje o wykorzystanych danych walidacyjnych i danych testowych oraz ich głównych cechach; wskaźniki stosowane do pomiaru dokładności, solidności, cyberbezpieczeństwa i zgodności z innymi stosownymi wymogami określonymi w niniejszych klauzulach, jak również potencjalnie dyskryminujących skutków; rejestry zdarzeń generowane podczas testów i wszystkie sprawozdania z testów opatrzone datą i podpisane przez osoby odpowiedzialne, w tym w odniesieniu do z góry zaplanowanych zmian, o których mowa w pkt 2.5;
 - 2.7. wdrożone środki cyberbezpieczeństwa.

Szczegółowe informacje dotyczące monitorowania, funkcjonowania i kontroli systemu sztucznej inteligencji, w szczególności w odniesieniu do: jego możliwości i ograniczeń w zakresie skuteczności działania, w tym stopnie dokładności w przypadku określonych osób lub grup osób, względem których system ma być wykorzystywany, oraz ogólny spodziewany poziom dokładności w stosunku do jego przeznaczenia; możliwych do przewidzenia niezamierzonych wyników działania i źródeł zagrożeń dla zdrowia i bezpieczeństwa, praw podstawowych i dyskryminacji w świetle przeznaczenia systemu sztucznej inteligencji.

3. Szczegółowy opis systemu zarządzania ryzykiem zgodnie z art. 2.
4. Opis wszelkich istotnych zmian, których dostawca dokonał w systemie w jego cyklu życia.

Załącznik D Instrukcja obsługi

Instrukcja obsługi musi zawierać, stosownie do przypadku, co najmniej następujące informacje właściwe dla systemu sztucznej inteligencji:

1. Tożsamość i dane kontaktowe dostawcy oraz, w stosownych przypadkach, jego upoważnionych przedstawicieli.
2. Cechy, możliwości i ograniczenia skuteczności działania systemu sztucznej inteligencji, w tym, w stosownych przypadkach:
 - 2.1. przeznaczenie;
 - 2.2. poziom dokładności, solidności i cyberbezpieczeństwa, o którym mowa w art. 8, względem którego przetestowano system sztucznej inteligencji i dokonano jego walidacji oraz którego można oczekiwać, a także wszelkie powszechnie znane i dające się przewidzieć okoliczności, które mogą mieć wpływ na ten oczekiwany poziom dokładności, solidności i cyberbezpieczeństwa;
 - 2.3. wszelkie powszechnie znane lub dające się przewidzieć okoliczności związane z wykorzystaniem systemu sztucznej inteligencji zgodnie z jego przeznaczeniem lub w warunkach dającego się racjonalnie przewidzieć niewłaściwego wykorzystania, które mogą powodować zagrożenia dla zdrowia i bezpieczeństwa lub praw podstawowych;
 - 2.4. stopień, w jakim system sztucznej inteligencji może wyjaśniać podejmowane przez siebie decyzje;
 - 2.5. skuteczność działania systemu w odniesieniu do osób lub grup osób, względem których system sztucznej inteligencji ma być wykorzystywany;
 - 2.6. istotne informacje na temat działań użytkowników, które mogą mieć wpływ na skuteczność działania systemu, w tym rodzaj lub jakość danych wejściowych lub wszelkie inne istotne informacje dotyczące wykorzystywanych zbiorów danych treningowych, walidacyjnych i testowych, uwzględniając przeznaczenie systemu sztucznej inteligencji.
3. Ewentualne zmiany w systemie sztucznej inteligencji i jego skuteczności działania, które zostały z góry zaplanowane przez dostawcę.
4. Środki sprawowania nadzoru przez człowieka, o których mowa w art. 7, w tym środki techniczne wprowadzone w celu ułatwienia organizacji publicznej interpretacji wyników działania systemu sztucznej inteligencji.
5. Przewidywany cykl życia systemu sztucznej inteligencji oraz wszelkie niezbędne środki w zakresie konserwacji i utrzymania mające na celu zapewnienie właściwego funkcjonowania tego systemu sztucznej inteligencji, w tym dotyczące aktualizacji oprogramowania.
6. Opis zawartych w systemie sztucznej inteligencji mechanizmów, które umożliwiają użytkownikom właściwe gromadzenie, przechowywanie i interpretowanie rejestrów zdarzeń.

Załącznik E Środki zapewniające przejrzystość

W tym miejscu proszę opisać środki techniczne i organizacyjne, które dostawca ma wprowadzić w celu zapewnienia przejrzystości zgodnie z art. 6 klauzul.

Załącznik F Środki zapewniające sprawowanie nadzoru przez człowieka

W tym miejscu proszę opisać środki techniczne i organizacyjne, które dostawca ma wprowadzić w celu zapewnienia sprawowania nadzoru przez człowieka zgodnie z art. 7 klauzul.

Załącznik G Poziomy dokładności

W tym miejscu proszę opisać wymagane poziomy dokładności.

Załącznik H Środki zapewniające odpowiedni poziom solidności, bezpieczeństwa i cyberbezpieczeństwa

W tym miejscu proszę opisać środki techniczne i organizacyjne, które dostawca ma wprowadzić w celu zapewnienia odpowiedniego poziomu solidności, bezpieczeństwa i cyberbezpieczeństwa zgodnie z art. 8 klauzul.

Środki te muszą zapewnić jak największą odporność systemu sztucznej inteligencji na błędy, usterki lub niespójności, które mogą wystąpić w systemie lub w środowisku, w którym działa system, w szczególności w wyniku interakcji z osobami fizycznymi lub innymi systemami.

System sztucznej inteligencji musi być odporny na podejmowane przez nieupoważnione osoby trzecie próby modyfikacji jego zastosowania, zachowania, wyników lub skuteczności działania poprzez wykorzystanie słabych punktów systemu. Rozwiązania techniczne mające na celu eliminowanie podatności charakterystycznych dla sztucznej inteligencji mogą obejmować, w stosownych przypadkach, środki służące zapobieganiu: atakom mającym na celu manipulowanie zbiorem danych treningowych („data poisoning”) lub wcześniej wytrenowanymi elementami wykorzystanymi w procesie trenowania („model poisoning”), danym wejściowym, które mają na celu spowodowanie błędu w modelu („niepożądane przykłady” lub „model evasion”), atakom naruszającym poufność lub wadom modelu, które mogą prowadzić do podejmowania szkodliwych decyzji, a także środki służące wykrywaniu tych zagrożeń, reagowaniu na nie, ich eliminowaniu oraz weryfikacji działania systemu pod ich kątem.