|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| ***Nazwa dokumentu: Rekomendacje uzycia generatywnej AI w adm. publicznej do konsultacji (5070817).docx*** | | | | | |
| **Lp.** | **Organ wnoszący uwagi** | **Jednostka redakcyjna, do której wnoszone są uwagi** | **Treść uwagi** | **Propozycja zmian zapisu** | **Odniesienie do uwagi** |
|  | **MRPiPS** | Cały dokument | Dokument wymaga korekty językowej: wiele zapisów jest niezrozumiałych, zawiera błędy stylistyczne i gramatyczne.  Ponadto, jest mało przejrzysty, zawiera powtórzenia podobnych treści, za dużo śródtytułów (na niebiesko) i potem b. krótkie rozwinięcia. | Dokument powinien przyjąć formę krótkiej ulotki np. 2-stronnicowej i w kilku blokach skrótowo zawrzeć główne myśli | Uwzględniono |
|  | **MRPiPS** | Str. 2 Wstęp | Należy przeformułować zdanie:  Ostatnia część jest najbardziej techniczna i opisuje rekomendacje użycia GenAI zależnie od modelu dostępu oraz dalsze technologiczne rekomendacje, które warto wziąć pod uwagę przy wyborze systemów sztucznej inteligencji do użycia i zakupienia do urzędu. | Ostatnia część podręcznika dotyczy technologii i opisów użycia GenAI w zależności od modelu, które warto wziąć pod uwagę przy ew. zakupie systemu sztucznej inteligencji. | Nie uwzględniono. Dokument w zamyśle skierowany jest do osób nieznających się na opisywanej tematyce. Ma mieć charakter pierwszego przewodnika dla pracowników administracji publicznej, którzy wcześniej nie mieli do czynienia z GenAI. Kwestie technologiczne będą omówione w obszerniejszym zbiorze wytycznych dla Urzędów. (w przygotowaniu). |
|  | **MRPiPS** | Str. 3 Czym jest generatywna sztuczna inteligencja? | Wprowadzić korektę tekstu  Najczęściej używane narzędzia generatywnej AI w odpowiedzi na polecenie generują teksty, obrazy albo filmy. | Najczęściej używane narzędzia generatywnej AI w odpowiedzi na wydane polecenie generują teksty, obrazy albo filmy. | Uwzględniono. |
|  | **MRPiPS** | Str. 4 Przykład nr 1: Źródło inspiracji | Fragment: „Należy pamiętać, aby sprawdzać czy wygenerowane pomysły nie są błędne, stronnicze lub dyskryminujące”. Wymaga uzupełnienia. | Należy wskazać rekomendację, w jaki sposób sprawdzić iż wygenerowane pomysły nie są błędne, stronnicze lub dyskryminujące. | Uwzględniono. |
|  | **MRPiPS** | Str. 5 Precyzyjny kontekst | Na przykład: Poinformuj GenAI, że jest się pracownikiem konkretnej instytucji, np. kuratorium oświaty. Wyjaśniając, że zadaniem programu jest sprawdzenie w jaki sposób aktualnie obowiązujący system ocen w polskich szkołach pozwala na weryfikację rzeczywistych postępów ucznia w nauce. | Na przykład: Poinformuj GenAI, że jesteś pracownikiem konkretnej instytucji, np. kuratorium oświaty. Wyjaśniając, że oczekujesz sprawdzenia w jaki sposób aktualnie obowiązujący system ocen w polskich szkołach pozwala na weryfikację rzeczywistych postępów ucznia w nauce. | Częściowo uwzględniono |
|  | **MRPiPS** | Str. 6 Prosić o przykłady i podawać informacje dodatkowe | Wykorzystany przykład wymaga korekty  Należy również informacje zwrotne – podtrzymywać wymianę informacji („rozmowę”) . Jeżeli otrzymana z narzędzia nie jest satysfakcjonująca | Należy również wykorzystać informacje zwrotne – podtrzymywać wymianę informacji („rozmowę”) . Jeżeli przygotowane odpowiedź przez narzędzie nie jest satysfakcjonująca | Częściowo uwzględniono |
|  | **MRPiPS** | Str. 12 System godny zaufania | W punkcie b) efektywnego nadzoru człowieka . | Należy rozwinąć ten zapis biorąc pod uwagę wykonywanie zadań w urzędzie na poszczególnych szczeblach w hierarchii zawodowej. To, co za pomocą AI stworzy pracownik nie powinno ujrzeć „światła dziennego” bez akceptacji przełożonego. System powinien być tak skonstruowany aby tworzyć blokadę. | Nie uwzględniono. |
|  | **MRPiPS** | Str. 12 | Dodać rekomendacje ogólne | W rekomendacjach ogólnych wskazać, iż podstawową korzyścią z korzystania z narzędzi GenAI w urzędach, może być automatyzowanie wielu procedur stosowanych przez urzędnika, a tym samym zwiększenie efektywności jego pracy | Nie uwzględniono. Dokument w zamyśle skierowany jest do osób nieznających się na opisywanej tematyce. Ma mieć charakter wprowadzenia pracowników administracji publicznej, którzy wcześniej nie mieli do czynienia z GenAI w podstawowe zagadnienia. Kwestie możliwości automatyzowania procedur stosowanych przez urzędników będą rozważone przy tworzeniu zbioru wytycznych dla Urzędów. (w przygotowaniu). |
|  | **GUS** | Dotyczy całości dokumentu | Proponuje się dodać numerację nagłówków (tytułów rozdziałów/podrozdziałów). | Nie dotyczy | Nie uwzględniono |
|  | **GUS** | Dotyczy całości dokumentu | Dokument powinien zostać prawidłowo zredagowany, w szczególności pod kątem poprawności gramatycznej, brakujących słów, powtórzeń, itp. | Nie dotyczy | uwzględniono |
|  | **GUS** | Rozdział „W skrócie: o czym pamiętać korzystając z GenAI w celach służbowych” (str.3)  Rozdział „O czym należy pamiętać, korzystając z GenAI w celach służbowych” | Proponuje się połączenie obu rozdziałów. Brak uzasadnienia dla wydzielania osobnego streszczenia. | Nie dotyczy | uwzględniono |
|  | ZUS | Uwaga ogólna | Dokument skupia się na sposobie korzystania z narzędzi wykorzystujących generatywną sztuczną inteligencję działającą w ramach publicznie dostępnych w Internecie usług (lub wywołujących te usługi w ramach systemów wewnętrznych instytucji). Należy wskazać, że możliwe są rozwiązania, w których generatywna sztuczna inteligencja jest rozwiązaniem prywatnym danej  instytucji/sfery publicznej i dla tego typu rozwiązań mogą obowiązywać inne  rekomendacje. Należy również wskazać, że każda instytucja może mieć własne wewnętrzne regulacje i rekomendacje związane z użytkowaniem AI. |  | Nie uwzględniono. Dokument dotyczy tylko korzystania z narzędzi powszechnie dostępnych. |
|  | ZUS | Uwaga ogólna | Głównym przedmiotem rekomendacji jest sposób korzystania z modeli językowych. Obecnie na rynku dostępne są rozwiązania związane z przetwarzaniem dźwięku, grafiki, video etc. Proponuję weryfikację dokumentu pod kątem uzupełnienia rekomendacji w kontekście tych bardziej specjalizowanych zastosowań generatywnej sztucznej inteligencji. |  | Nie uwzględniono. Dokument stanowi wprowadzenie do korzystania z GenAI na poziomie podstawowym. W zamyśle skierowany jest do osób nieznających się na opisywanej tematyce. W przygotowaniu obszerniejszy przewodnik - - zbiór wytycznych dla Urzędów. |
|  | ZUS | Uwaga ogólna | Celem Poradnika jest wsparcie pracowników sektora publicznego w minimalizacji ryzyka niewłaściwego i potencjalnie szkodliwego wykorzystania GenAI. Aby osiągnąć ten cel, ważnym jest, aby pracownik korzystający z możliwości wsparcia GenAI miał świadomość, że działa zgodnie z przepisami prawa. Stąd proponujemy, aby rozszerzyć Poradnik o informacje, jakie obowiązują (lub będą obowiązywać od najbliższego czasu) uregulowania prawne w tym zakresie – zarówno na poziomie prawa europejskiego, jak i krajowego – zawierające wykładnię tych przepisów. |  | j.w. |
|  | ZUS | Uwaga ogólna | Elementem ułatwiającym podjęcie decyzji, czy można wykorzystywać do realizacji zadań GenAI byłyby również przykłady odnoszące się do zadań realizowanych przez administrację publiczną – z uwzględnieniem, jeżeli jest taka możliwość, sytuacji, w których wykorzystanie GenAI jest niedozwolone. |  | j.w. |
|  | ZUS | Uwaga ogólna | Czy użyte sformułowanie (str. 7 i str. 10 dokumentu) „informacje niejawne” należy ściśle interpretować pod kątem ustawy o ochronie informacji niejawnych, czy też szeroko jako informacje zakwalifikowane do nieujawniania.  Niniejsza wątpliwość wynika z faktu, iż z ww.  ustawy usunięto podział informacji, który wyodrębniał m.in. „tajemnicę służbową”, a więc brak jawności należy obecnie kwalifikować głównie poprzez ocenę interesów Państwa. Natomiast instytucje wchodzą w posiadanie informacji (dokumentów) np. stanowiących Tajemnicę przedsiębiorstwa lub niemożliwych do ujawnienia do pewnego etapu w procesie – co reguluje konkretny akt prawny – zatem takich informacji - całkowicie lub w pewnym określony czasokresie - również nie należy wpisywać, stąd pytanie, czy nie należałoby doprecyzować takich okoliczności w opiniowanym akcie. |  | Nie uwzględniono. Dokument w zamyśle skierowany jest do osób nieznających się na opisywanej tematyce. Ma mieć charakter „ściągawki” dla pracowników administracji publicznej, którzy wcześniej nie mieli do czynienia z GenAI.  W przygotowaniu obszerniejszy przewodnik - - zbiór wytycznych dla Urzędów. |
|  | ZUS | Czym jest generatywna sztuczna inteligencja? | Generatywna sztuczna inteligencja ma możliwość generowania nowych instancji danych w różnych typach - nie tylko tekstowych, czy wizualnych. Z punktu widzenia statystycznych procesów analizy danych należy zwrócić uwagę, że GenAI jest również używana do wytwarzania „sztucznych danych” (ang. „synthetic data”) – czyli nierzeczywistych zestawów danych nie opartych na zdarzeniach świata rzeczywistego. Dane te tworzone są algorytmicznie i używane do walidacji i trenowania modeli uczenia maszynowego w sytuacjach, gdy dane rzeczywiste nie mogą być dostępne. |  | j.w. |
|  | ZUS | Czym jest generatywna sztuczna inteligencja? | Po zapewnianiu odpowiednich baz referencyjnych oraz zbudowaniu powiązań referencyjnych AI może wykonać wiele czynności oraz pozwala użytkownikom tworzyć nowe treści cyfrowe takie jak teksty, obrazy(filmy), aplikacje, bazy danych. |  | j.w. |
|  | ZUS | W skrócie: o czym pamiętać korzystając z GenAI w celach służbowych | Należy zwrócić uwagę, że GenAI nie jest dostępna wyłącznie w sposób jawny, wymagający świadomej decyzji użytkownika o jej użyciu. Coraz częściej mamy do czynienia z tzw. wbudowaną GenAI (ang. embedded GenAI), gdzie funkcjonalności GenAI są implementowane bezpośrednio w „codzienne” oprogramowanie  (procesory tekstu, arkusze kalkulacyjne, aplikacje biznesowe itp.) i nie ma oczywistej granicy miedzy funkcjonalnościami nie wykorzystującymi GenAI i korzystającymi z GenAI – co znacząco utrudnia mitygację ryzyk opisanych dalej w dokumencie. |  | j.w.. |
|  | ZUS | W skrócie: o czym pamiętać korzystając z GenAI w celach służbowych | Jeżeli jest to poradnik dla pracowników administracji to warto rozważyć dodanie informacji, że przy wykorzystaniu AI w organizacji należy również stosować się do zasad określonych w danych urzędzie/instytucji. |  | Uwzględniono. |
|  | ZUS | W skrócie: o czym pamiętać korzystając z GenAI w celach służbowych | Przy zdaniu „Nie należy wprowadzać do takich narzędzi informacji lub dokumentów…” do rozważenia dodanie w tym miejscu i na końcu dokumentu punktu odnoszącego się do informacji o stosowanych zabezpieczeniach. Co prawda można to podciągnąć pod inne hasło, ale może warto zasygnalizować? |  | Nie uwzględniono.  Kwestie zabezpieczeń będą szczegółowo rozważane w zbiorze wytycznych dla Urzędów. (w przygotowaniu).  Ten dokument w zamyśle skierowany jest do osób nieznających się na opisywanej tematyce. Ma mieć charakter „ściągawki” dla pracowników administracji publicznej. |
|  | ZUS | Jak Generatywna Sztuczna Inteligencja może pomóc w pracy? | Można rozszerzyć listę przykładów o inne możliwe aspekty wykorzystania GenAI. | Przykład nr 5. Generowanie kodu źródłowego nowego oprogramowania. GenAI może być pomocna w tworzeniu i  rozwijaniu elementów oprogramowania, zarówno poprzez wykorzystanie zaproponowanych przez GenAI bloków kodu, jak i weryfikacji istniejących (wytworzonych przez człowieka). Przykład nr 6. Analiza danych. GenAI może być wykorzystywana w eksploracji danych (np. tworzenie hipotez badawczych na podstawie danych, automatyzacja testowania hipotez), pomocna w generowaniu kodu oprogramowania statystycznego, czy tworzenia teksów podsumowań badań i analiz. Część aplikacji analiz danych obsługuje tzw. „interfejsy konwersacyjne” wykorzystywane do wykonywania analiz bez znajomości kodowania, czy wykorzystania zaawansowanych klasycznych funkcji programów. Przykład nr 7. Gen AI może być wykorzystana do wykonania analiz w zakresie wyboru spraw do weryfikacji uprawnień dla celów zwalczania nadużyć w zakresie świadczeń i właściwego ustawodawstwa (wdrożenie rozwiązań antyfraudowych) | Nie uwzględniono.  Propozycje będą rozważone przy tworzeniu zbioru wytycznych dla Urzędów (w przygotowaniu). |
|  | ZUS | Jaki wybrać i przygotować system? | Propozycja do rozważenia dodania do dokumentu zapisu o konieczności sporządzenia przed wdrożeniem jakiejkolwiek aplikacji lub systemu opartego na generatywnej sztucznej inteligencji zalecenia przeprowadzenia Oceny Skutków dla Ochrony Danych, tak aby zidentyfikować cele i kontekst, przeanalizować ryzyka i zagrożenia, upewnić się, że przetwarzanie danych będzie zgodne z obowiązującymi przepisami o ochronie danych osobowych i wprowadzić odpowiednie środki bezpieczeństwa, aby minimalizować ryzyko naruszenia danych. |  | Nie uwzględniono.  Kwestie zabezpieczeń będą szczegółowo rozważane przy tworzeniu zbioru wytycznych dla Urzędów (w przygotowaniu). |
|  | **MSWiA** | **Wstęp**  str. 2  Chcąc zaadresować tę kwestię Ministerstwo Cyfryzacji przygotowało ten poradnik.  Mając świadomość tempa rozwoju technologii AI, wytyczne będą poddawane regularnemu przeglądowi. | Poradnik, rekomendacje, wytyczne – pod rozwagę uspójnienie terminologii i posługiwanie się jednym terminem na potrzeby dokumentu. Może tym, który został wskazany w tytule tj. rekomendacje.  Ponadto pod rozwagę dodanie, że nie mają one wiążącego charakteru, o ile tak jest. |  | Uwzględniono. |
|  | **MSWiA** | **W skrócie: o czym pamiętać korzystając z GenAI w celach służbowych**  str. 3 | Zanim umożliwi się pracownikom skorzystanie  z rozwiązań AI, to w pierwszej kolejności powinny one zostać poddane weryfikacji przez specjalistów w dziedzinie AI i systemowo zostać zarekomendowane dla administracji np.  w postaci konkretnych programów, produktów, usług itp.  Nie należy przerzucać odpowiedzialności na najniższy szczebel – „rekomendując” jedynie dane narzędzie.  Większość dostępnych obecnie generatywnych modeli AI działa w chmurze. Także w chmurach nie podlegających jurysdykcji polskiej, czy jurysdykcji państwa członkowskiego Unii Europejskiej. Zwykle chmury te nie są także  w stanie zagwarantować prawa właściciela do swojej informacji. Należy mieć na uwadze, że  w przypadku korzystania z takich rozwiązań urząd administracji publicznej traci prawa do wytworzonych w ten sposób informacji. Informacji, które mogą być informacjami istotnymi dla realizacji zadań statutowych instytucji administracji publicznej.  W kontekście tworzenia zapytań do publicznych LLM, proponuje się uwzględnienie w wyliczeniu kategorii informacji niepodlegających upublicznieniu, które mogą dotyczyć m.in. np:  szczegółów lub podatności infrastruktury IT podmiotu  elementów polityk bezpieczeństwa podmiotu lub treści korespondencji wewnętrznej podmiotu (w kontekście redagowania treści przez AI), | „Nie należy wprowadzać do takich narzędzi informacji lub dokumentów, które:   * są niejawne lub zawierają dane wrażliwe. * zawierają informacje urzędowe będące w fazie przygotowawczej, a tym samym nie przeznaczone do upublicznienia; * naruszają przepisy o ochronie danych osobowych. * **ujawnione mogą doprowadzić do podniesienia poziomu ryzyk związanych z bezpieczeństwem informacji i cyberbezpieczeństwem.”.** | Nie uwzględniono.  Kwestie zabezpieczeń będą szczegółowo omówione w przy tworzeniu zbioru wytycznych dla Urzędów (w przygotowaniu).  Uwzględniono |
|  | **MSWiA** | **Jak Generatywna Sztuczna Inteligencja może pomóc w pracy?**  str. 4 | Czy lista bezpiecznych programów GenAI będzie dostępna, w szczególności tych, które pozwalają na uzyskanie poniższych propozycji zastosowania GenAI?  W jaki konkretnie sposób pracownik ma sprawdzić czy wygenerowane pomysły nie są błędne, stronnicze lub dyskryminujące? Czy zostanie przygotowane jakieś wsparcie jak to sprawdzać? Czy pracownik ma się zdać na własną ocenę, intuicję?  Warto zwrócić uwagę na problem stronniczości AI, który w głównej mierze powstaje na etapie projektowania i tworzenia. Pracownik na etapie stosowania może nawet nie być świadom tego, że wynik zapytania wyszedł stronniczy, błędny lub dyskryminujący. Dlatego rozwiązania, które zostaną zaproponowane pracownikom powinny zostać zweryfikowane przez specjalistów  w dziedzinie AI. |  | Nie uwzględniono.  Propozycje będą rozważane przy tworzeniu zbioru wytycznych dla Urzędów (w przygotowaniu). |
|  | **MSWiA** | **Jak prowadzić konstruktywną „rozmowę” z GenAI**  **Precyzyjny kontekst**  str. 5-6 | Przykład: *„Poinformuj GenAI, że jest się pracownikiem konkretnej instytucji…”.*  Kontekst oczywiście jest ważny dla tego typu rozwiązań, ale w ramach różnego rodzaju szkoleń zwraca się uwagę na to, aby pracownicy  z rozsądkiem podchodzili do ujawniania informacji o sobie oraz o miejscu pracy. Wynika to z rosnącej liczby zagrożeń związanych  z wyłudzeniami danych, oszustwami, phishingu, vishingu. Może zatem dojść do sytuacji w której będziemy mu rekomendowali sprzeczne zalecenia.  Dopóki nie zostanie opracowana zweryfikowana lista programów/rozwiązań/narzędzi, z której będą mogli korzystać pracownicy administracji, to nie możemy sobie tym zakresie pozwolić na dowolność. W gruncie rzecz większość z tych rozwiązań, to rozwiązania komercyjne, co do których pracownicy nie mają wiedzy w jaki sposób przetwarzane są w nich informacje, gdzie  i czy w ogóle przechowywane oraz do czego potencjalnie mogą zostać wykorzystane np.  w wyniku cyberataku na dostawcę takiego rozwiązania.  W związku z powyższym proponuje się zmianę treści porad dotyczących pisania promptów  w zakresie rekomendowania zachowania maksymalnej anonimowości w zapytaniach kierowanych do publicznych GenAI, dotyczących danych osobowych jak i informacji o instytucji.  Część modeli językowych jest uczona na podstawie wprowadzonych zapytań co może skutkować zbieraniem wewnętrznych danych  o Podmiocie przez osoby nieupoważnione, cyberprzestępców lub obce służby. | W przykładzie proponuje się wykreślenie zdania „Poinformuj GenAI, że jest się pracownikiem konkretnej instytucji, np. kuratorium oświaty.” | Uwzględniono. |
|  | **MSWiA** | **Jak prowadzić konstruktywną „rozmowę” z GenAI**  **Określenie wymaganego tonu i stylu?**  str. 6 | *„Można także poprosić o wygenerowanie mniej formalnego emaila na zadany temat, kierowanego do współpracowników. W zależności od zadania, do polecenia można dołączyć (wkleić) przyjęty w danym urzędzie tekstowy szablon dokumentu lub przykład struktury i języka tekstu, na bazie którego tworzony jest materiał.”*  W tym kontekście pod rozwagę należy poddać określenie katalogu spraw/wątków, w których tego typu pomoc mogłaby mieć zastosowanie, bez narażania się pracownika na udostępnienia wrażliwych informacji do takiego narzędzia/programu/usługi.  Pod rozwagę poddaje się jednak wskazanie jakie szablony dokumentów mogą być „dołączone” – wklejone. |  | Nie uwzględniono |
|  | **MSWiA** | **O czym należy pamiętać, korzystając z GenAI w celach służbowych**  str. 7 | „*Wchodząc w interakcję z wybranym narzędziem GenAI należy zachować podstawowe* [*zasady higieny cyfrowej*](https://www.gov.pl/web/baza-wiedzy/cyberbezpieczenstwo)*.”*  Pod rozwagę poddaje się wskazanie zasad higieny cyfrowej. |  | Uwzględniono |
|  | **MSWiA** | **O czym należy pamiętać, gdy wchodzi się w interakcję z GenAI - zwłaszcza w celach służbowych?**  **Ochrona danych**  str. 7-8 | *„Korzystając z jednego z popularnych ogólnodostępnych modeli językowych,* ***nie mamy kontroli nad danymi****, które są mu przekazywane.”*  Pod rozwagę poddaję się nie skupianie się tylko na popularnych rozwiązaniach, bo ten rynek szybko się rozwija.  Zgodnie z Art. 2 pkt 1 Dyrektywy Parlamentu Europejskiego i Rady (UE) 2016/943 z dnia 8 czerwca 2016 r. w sprawie ochrony niejawnego know-how i niejawnych informacji handlowych (tajemnic przedsiębiorstwa) przed ich bezprawnym pozyskiwaniem, wykorzystywaniem i ujawnianiem pod pojęciem "tajemnica przedsiębiorstwa" rozumie się „informacje, które spełniają wszystkie następujące wymogi: a) są poufne w tym sensie, że jako całość lub w szczególnym zestawie i zbiorze ich elementów nie są ogólnie znane lub łatwo dostępne dla osób  z kręgów, które zwykle zajmują się tym rodzajem informacji; b) mają wartość handlową dlatego, że są objęte tajemnicą; c) poddane zostały przez osobę, która zgodnie z prawem sprawuje nad nimi kontrolę, rozsądnym, w danych okolicznościach, działaniom dla utrzymania ich  w tajemnicy”.  Jest to zakres znacznie szerszy, niż zakres informacji opisanych w rekomendacjach, jako dane wymagające ochrony.  Tymczasem, podczas korzystania z rozwiązań GenAI może dość do przekazywania informacji spełniających wymogi "tajemnicy przedsiębiorstwa" jako elementów zapytań. Nie musi to tylko dotyczyć informacji urzędowych będących w fazie przygotowawczej, jak wskazują to rekomendacje. | Pod rozwagę modyfikacja na: „Korzystając  z ogólnodostępnych modeli językowych….”  Wskazane jest, by rozszerzony został katalog informacji uznanych, za informacje istotne dla realizacji działań statutowych instytucji administracji publicznej, udostępniane bez ograniczeń pracownikom instytucji lub na podstawie porozumień o zachowaniu poufności, które powinny podlegać ochronie.  Brak jest także wskazania wymaganej prawem ochrony dla danych stanowiących dane referencyjne krajowych rejestrów, które są określone w odrębnych przepisach (w tym np. dane  o kluczowym znaczeniu dla bezpieczeństwa publicznego). | Nie uwzględniono.  Propozycje będą rozważane przy tworzeniu zbioru wytycznych dla Urzędów (w przygotowaniu). |
|  | **MSWiA** | **Halucynacje**  str. 8 | *„Dlatego* ***zawsze należy weryfikować informacje uzyskane od modeli językowych.”***  Większość urzędów nie posiada specjalistów  w zakresie AI, więc będzie to zalecenie trudne do realizacji. Chyba, że zostanie administracji zalecone jakieś narzędzie do np. factchecingu.  ***„****Dlatego zawsze należy weryfikować materiały uzyskane z GenAI pod* ***względem ich reprezentatywności i bezstronności.”***  Pracownik na etapie stosowania może nawet nie być świadom tego, że wynik zapytania wyszedł stronniczy. Dlatego rozwiązania które zostaną zaproponowane pracownikom powin. ny zostać zweryfikowane przez specjalistów w dziedzinie AI. |  | Nie uwzględnione. |
|  | **MSWiA** | **Manipulacja**  str. 8 | *„Dlatego zawsze należy weryfikować zgodność z oryginałem, nie przyczyniać się do rozpowszechniania dezinformacji i* ***oznaczać, że stworzone treści są wygenerowane za pomocą sztucznej inteligencji.”***  To zbyt ogólne zalecenia. Jakimi narzędziami na to być sprawdzane? Jak ma taki materiał być oznaczony? Powinno to zostać określone odgórnie i jednolicie w ramach administracji publicznej. |  | Nie uwzględniono.  Propozycje będą rozważane przy tworzeniu zbioru wytycznych dla Urzędów (w przygotowaniu). |
|  | **MSWiA** | **Rekomendacje użycia GenAI w zależności od modelu dostępu**  str. 9-10 | Proponuje się rekomendować rozwiązania  on-premise  (wdrożenia lokalne). Ewentualny dostęp do chmury z dedykowanym dostępem będzie możliwy na zasadach i warunkach określonych  w Standardach Cyberbezpieczeństwa Chmur Obliczeniowych (SCOO) v.1.00.  Komercyjne usługi GenAI w chmurze bez dedykowanego dostępu stanowią zagrożenie udostępniania poufnych danych ze względu na specyfikę korzystania z tego typu narzędzi, zgodnie z uwagą pkt 2. |  | Nie uwzględniono.  Kwestie techniczne będą szczegółowo omówione w zbiorze wytycznych dla Urzędów (w przygotowaniu). |
|  | **MSWiA** | **Rozdział: „Cyberbezpieczeństwo”**  str. 12 | Proponuje się rozważenie dopisania do punktu 2 w celu informacyjnym również innych ataków ukierunkowanych na AI i LLM opisanych przez organizacje Mitre.org zajmującą się cyberbezpieczeństwem, albo wskazanie poniższego źródła. Matryca: https://atlas.mitre.org/matrices/ATLAS | Środowisko modelu powinno być zabezpieczone w celu uniemożliwienia ataków typu reverse-engineering, data-poisoning czy DDoS, także ataków ukierunkowanych na LLM opisanych przez organizację Mitre.org <https://atlas.mitre.org/matrices/ATLAS>. | Nie uwzględniono.  Kwestie będą szczegółowo rozważane przy tworzeniu zbioru wytycznych dla Urzędów (w przygotowaniu). |
|  | **MSWiA** | **System godny zaufania** str. 12 | Użyto sformułowania „user experience”.  Do wyjaśnienia – urzędowym językiem jest j. polski a nie j. angielski |  | Uwaga będzie uwzględniona przy tworzeniu zbioru wytycznych dla Urzędów (w przygotowaniu). |
|  | **MSWiA** | **Rozdział „Rekomendacje technologiczne”** Str. 12 | Proponuje się dodanie zalecenia stosowania modeli z popularnych i uznanych w środowisku open-source źródeł (np. Ollama.com, pllum.org.pl itp.). Modele przygotowane przez twórców o niskiej reputacji lub cyerprzestepców mogą propagować dezinformację lub generować niecenzuralne treści.  Do wyjaśnienia pojęcia użyte w języku angielskim (glass-box, black-box) – urzędowym językiem jest j. polski a nie j. angielski. | „Należy używać modeli na licencji typu open-source zamiast technologii zamkniętych, przy czym należy używać modeli z popularnych i uznanych w społeczności open-source źródeł. | Nie uwzględniono.  Kwestie technologiczne będą szczegółowo rozważane przy tworzeniu zbioru wytycznych dla Urzędów (w przygotowaniu). |
|  | **MZ** | Cały dokument | W dokumencie używa się wymiennie pojęć:  Urzędnik administracji publicznej  Pracownik administracji publicznej  Pracownik sektora publicznego  Powyższe pojęcia nie są tożsame. | W zależności od intencji w zakresie grupy docelowej, należy ujednolicić terminologię, w naszej ocenie optymalnie do: pracownik administracji publicznej. | Uwzględniono. |
|  | **MZ** | Cały dokument | Liczne wystąpienia specjalistycznych pojęć, np.  Black-box/ glass-box, retrenowanie modelu, reverse-engineering, data-poisoning, DDoS.  Dokument zgodnie z tytułem jest przeznaczony do szerokiego grona odbiorców, dla którego część pojęć może być niezrozumiała. | Dodanie słowniczka najważniejszych pojęć na początku dokumentu. | Częściowo uwzględniono – usunięto niezrozumiałe specjalistyczne pojęcia. Dokument w zamyśle skierowany jest do osób nieznających się na opisywanej tematyce. Ma mieć charakter „ściągawki” dla pracowników administracji publicznej, którzy wcześniej nie mieli do czynienia z GenAI. |
|  | **MNiSW** |  | Odnośnie do treści zawartej w przedstawionym projekcie, w szczególności w części zatytułowanej 'W skrócie: o czym pamiętać korzystając z GenAI w celach służbowych' (str. 3 projektu) oraz 'O czym należy pamiętać, korzystając z GenAI w celach służbowych' (str. 7 projektu) przedstawiam następujące uwagi.   1. Należy zauważyć, że ustawa z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych (Dz. U. z 2024 r. poz. 632) ujmuje wyrazy 'informacje niejawne' jako skrót, który jest wykorzystywany w ramach tej ustawy (art. 1 ust. 1 ww. ustawy). 2. Projektodawca nie wyjaśnia w przedstawionym projekcie co rozumie przez pojęcie 'danych wrażliwych' (str. 3 i 7), 'informacji urzędowych będących w fazie przygotowawczej' (str. 3), 'wewnętrznych informacji urzędowych, będących w fazie przygotowawczej' (str. 7), 'wewnętrznych informacji urzędowych' (str. 9), 'kontrolowanych wrażliwych danych urzędowych' (str. 9), ani 'kontrolowanych danych urzędowych' (str. 9).   Ponadto wskazanie, że nie należy wprowadzać do narzędzi GenAI 'informacji urzędowych, będących w fazie przygotowawczej, a tym samym nie przeznaczonych do upublicznienia' (str. 3 i 7) oraz nie należy wprowadzać do narzędzi GenAI w chmurze bez dedykowanego dostępu 'żadnych wewnętrznych informacji urzędowych, które nie są publicznie dostępne dla wszystkich obywateli i obywatelek', sugeruje możliwość wprowadzania do ww. narzędzi wyłącznie informacji stanowiących informacje publiczne i publikowanych w ogólnodostępnej sieci internet. Wydaje się, że stoi to w sprzeczności w określonymi przykładami bezpiecznego i zgodnego z zasadami zastosowania programów GenAI, gdzie wskazano m.in. wykorzystanie ww. narzędzia jako źródło inspiracji (są to bez wątpienia informacje będące w fazie przygotowawczej) lub jako tłumacz lub redaktor treści (wskazano na uzyskiwanie propozycji odpowiedzi na wiadomości mailowe). | Proponuje się użycie konstrukcji informacje niejawne w rozumieniu ustawy z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych lub pełnej nazwy dla określenia tego typu informacji;  Proponuje się dodać wyjaśnienie wskazanych pojęć;  W związku z powyższym proponuje się ponowną analizę zaproponowanego katalogu i określenie na nowo, zbioru informacji, których według przedmiotowych rekomendacji nie należy wpisywać do omawianych narzędzi; | Nie uwzględniono.  Propozycje będą rozważane przy tworzeniu zbioru wytycznych dla Urzędów (w przygotowaniu). |
|  | **MFiPR**  **DI** | Podrozdział:  „W skrócie: o czym pamiętać korzystając z GenAI w celach służbowych” | „Za każdym razem weryfikować ich rezultaty - narzędzia GenAI są podatne na stronniczość i dezinformację (tzw. *Halucynacje*)” | „Za każdym razem weryfikować ich rezultaty - narzędzia GenAI są podatne na stronniczość, dezinformację, halucynacje, manipulację, naruszenia własności intelektualnej oraz na ataki typu jailbreaking i wstrzyknięcia złośliwego kodu”.  Wszystkie wymienione zagrożenia powinny być krótko scharakteryzowane w podrozdziale „O czym należy pamiętać, gdy wchodzi się w interakcję z GenAI - zwłaszcza w celach służbowych? na str. 7” | Nie uwzględniono  Kwestie będą szczegółowo rozważane przy tworzeniu zbioru wytycznych dla Urzędów (w przygotowaniu). |
|  | **MFiPR**  **DI** | Pkt: „GenAI w chmurze bez dedykowanego dostępu” | „2. Nie należy wpisywać do takich narzędzi żadnych informacji niejawnych, kontrolowanych wrażliwych danych urzędowych ani kontrolowanych danych urzędowych (np. objętych RODO).” | Sformułowanie „kontrolowanych wrażliwych danych urzędowych ani kontrolowanych danych urzędowych” wymaga doprecyzowania. | Nie uwzględniono.  Kwestie technologiczne będą szczegółowo omówione w zbiorze wytycznych dla Urzędów (w przygotowaniu). |
|  | **MFiPR**  **DI** | Pkt „GenAI w chmurze z dedykowanym dostępem” | „2. Należy wpisywać tam tylko informacje jawne i nieobjęte kontrolą.” - podobnie jak to miało miejsce w poprzedniej uwadze doprecyzowania wymaga pojęcie „”informacji nieobjętych kontrolą. Wydaje się, że właściwym w tym przypadku sformułowanie będzie „informacje nieobjęte mechanizmami ochrony, klasyfikacja informacji, etykietowanie, itp.” | Wydaje się, że właściwym w tym przypadku sformułowaniem będzie „informacje nieobjęte mechanizmami ochrony, np. klasyfikacja informacji, etykietowanie, itp.” | Nie uwzględniono.  Kwestie technologiczne będą szczegółowo omówione w zbiorze wytycznych dla Urzędów (w przygotowaniu). |
|  | **MFiPR**  **DI** | Pkt  „Cyberbezpiecze ństwo” | „Wszystkie systemy sztucznej inteligencji wykorzystujące dane osobowe lub inne dane zawierające informacje o istotnym znaczeniu dla sektora publicznego powinny mieć zapewnione warunki:  a) solidności technicznej i najwyższego poziomu cyberbezpieczeństwa,” | Zapis wymaga doprecyzowania chociażby z faktu powołania się na dobre praktyki w zakresie modeli AI. | Nie uwzględniono.  Kwestie cyberbezpieczeństwa będą szczegółowo omówione w zbiorze wytycznych dla Urzędów (w przygotowaniu). |
|  | **MFiPR**  **DI** | Pkt  „Cyberbezpiecze ństwo” | „3. Retrenowanie modelu powinno odbywać się tylko na uporządkowanych danych zweryfikowanych statystycznie. | Sformułowanie wymaga doprecyzowania chociażby z faktu powołania się na dobre praktyki w zakresie modeli AI. | j.w. |
|  | **MFiPR**  **DI** | Pkt „System godny zaufania ” | W przywołanym punkcie nie wiadomo do końca – bez dodatkowego wyjaśnienia - czy wymienione tu wymagania są kryteriami stanowiącymi o systemie godnym zaufania? | Zapis wymaga dodatkowego wyjaśnienia. | j.w. |
|  | **MFiPR**  **DI** | Pkt „System godny zaufania ” | „4. Decyzje modelu powinny być szczegółowo wyjaśniane i powszechnie dostępne.” | Zapis wymaga dodatkowego wyjaśnienia co do celu takiego działania. | j.w. |
|  | **MFiPR BPB** | Uwaga ogólna | Proponujemy dopisanie informacji o wykorzystywaniu możliwości (nie we wszystkich przypadkach) skorzystania wyłącznie ze stron należących do administracji publicznej. Zastosowanie takiego modelu daje pewną gwarancję, iż tekst nie będzie stronniczy i nie będzie zawierał dezinformacji. |  | Uwaga niezrozumiała |
|  | **MF** | Str. 3 | „Pojawienie się i upowszechnienie takich narzędzi z stwarza możliwość ich zastosowania do powtarzalnych zadań służbowych”, str. 2  „Przy zachowaniu odpowiednich środków ostrożności, GenAI może pomóc wykonywać niektóre, rutynowe zadania służbowe.” | Ten fragment wstępu sugeruje, że GenAI może być wykorzystywane do automatyzacji procesów. W pewnych zastosowaniach jest to prawdziwe jak zbieranie informacji do procesów decyzyjnych (generowanie podsumowań), ale biorąc pod uwagę potencjalnego odbiorcę automatyzacja może być utożsamiania z robotyzacją.  Warto rozważyć usunięcie słowa „powtarzalne” i „rutynowe”. | Nie uwzględniono |
|  | **MF** | Str. 2 | „Rosnąca popularność takich narzędzi sprawia, że w praktyce są coraz częściej wykorzystywane przez pracowników - w tym urzędników administracji publicznej” | Z uwagi na różny zakres zadań publicznych konkretnych organów administracji publicznej warto rozważyć dodanie „w przypadku dopuszczenia stosowania przez dany resort, pracownicy…”. | Nie uwzględniono |
|  | **MF** | Str. 2 | „Rosnąca popularność takich narzędzi sprawia, że w praktyce są coraz częściej wykorzystywane przez pracowników -w tym urzędników administracji publicznej”,  „Poradnik składa się z części, które opisują kolejno: definicje i podstawowe terminy, przykłady zastosowań, jak również wskazówki dla pracowników administracji rządowej dotyczące tego, w jaki sposób bezpiecznie korzystać z narzędzi GenAI dla usprawnienia bieżącej pracy” | Warto rozważyć zamianę słowa urzędnik” na „pracownik”, z uwagi na fakt, że stosunek pracy może być nawiązany w różny sposób i nie każdy pracownik urzędu organu administracji publicznej jest urzędnikiem w ścisłym tego słowa znaczeniu. Warto również jednoznacznie określić grupę adresatów dokumentu albo w całości, lub też, z uwagi na szeroki spektrum poruszanych tematów, przy różnych częściach dokumentu, być może część z treści skierowana powinna być nie do pracowników merytorycznych, a developerów, bądź pracowników IT i zajmujących się bezpieczeństwem teleinformatycznym w resortach, z uwagi na fakt, że część pracowników meteorycznych nie posiada wiedzy, kompetencji i umiejętności pozwalających na weryfikację działania algorytmów oraz innych kwestii technicznych.  W dokumencie znajduje się określenie, że dokument dotyczy administracji rządowej, co zdecydowanie zawęża perspektywę względem pojęcia „administracja publiczna”. | Uwzględniono |
|  | **MF** | Str. 2 | „Chcąc zaadresować tę kwestię Ministerstwo Cyfryzacji przygotowało ten poradnik. Jego głównym celem, obok prezentacji tej technologii oraz jej użyteczności, wsparcie pracowników sektora publicznego w minimalizowaniu ryzyka niewłaściwego i potencjalnie szkodliwego wykorzystania GenAI.” | Sugerujemy „Mając na uwadze tę kwestię”, z uwagi na fakt, że zastosowana w tekście forma stanowi kalkę z języka angielskiego. | Uwzględniono |
|  | **MF** | Str. 2 | „Jego głównym celem, obok prezentacji tej technologii oraz jej użyteczności, wsparcie pracowników sektora publicznego w minimalizowaniu ryzyka niewłaściwego i potencjalnie szkodliwego wykorzystania GenAI” | W klasycznej definicji ryzyko może mieć również pozytywne konsekwencje, lecz powszechnie przyjmuje się, że ryzyko jest negatywne, w związku z tym sugerujemy usunąć „ potencjalnego”, ponieważ samo sformułowanie niewłaściwe nadaje kontekst „szkodliwe” dla ryzyka jako czegoś niezmaterializowanego. | Uwzględniono |
|  | **MF** | Str. 3 | „Te narzędzia określa się jako tzw. generatywną sztuczną inteligencję (dalej: GenAI)”, str, 2  „Najczęściej używane narzędzia generatywnej AI w odpowiedzi ...”, str. 3  „Algorytmy modeli generatywnej sztucznej inteligencji działają…” | Z uwagi na przejrzystość i przystępność tekstu dla odbiorcy wartościowe może być konsekwentnie korzystanie z wprowadzonego skrótu.  Warto równie z rozważyć wprowadzenie słownika na początku dokumentu definiującego podstawowe pojęcia celem wprowadzenia adresata w tematykę. | Częściowo uwzględniono |
|  | **MF** | Str. 3 | „Za każdym razem … narzędzia GenAI są podatne na stronniczość i dezinformację (tzw. *Halucynacje*)” | Halucynacje odnoszą się do generowania nieprawdziwych informacji, nie dezinformacji, która jest pojęciem różnym i węższym. | Uwzględniono |
|  | **MF** | Str. 3 | „W przypadku wykorzystania wyników w dalszej pracy, zawsze informować, że treści, które są przekazywane były stworzone lub przetworzone z wykorzystaniem narzędzi GenAI (np. oznaczać cytatem fragmenty wprost zaczerpnięty z takiego narzędzia)”,  „Należy pamiętać, aby sprawdzać czy wygenerowane pomysły nie są błędne, stronnicze lub dyskryminujące. Jeżeli wynik działania systemu ma być przekazany dalej, wskazane jest oznaczenie, które treści zostały przygotowane ze wsparciem sztucznej inteligencji” | Warto rozważyć zastosowanie rozwiązania stosowanego w świecie nauki – „Ten dokument powstał z wykorzystaniem genAI”. Ewentualnie poszerzyć o „Treści zostały zweryfikowane przez człowieka”. | Uwzględniono |
|  | **MF** | Str. , 7 | „GenAI to narzędzie z dużym potencjałem zastosowania, które przy zachowaniu należytej staranności może być pomocne w usprawnieniu realizowanych zadań”  „GenAI, jako system bazujący na rozpoznawaniu powtarzających się wzorców, bardzo dobrze radzi sobie z wymienianiem wariantów i proponowaniem alternatyw” | GenAI to definicyjnie dziedzina AI, nie system ani narzędzie. | Uwzględniono |
|  | **MF** |  | „Jak Generatywna Sztuczna Inteligencja może pomóc w pracy?”  „O czym należy pamiętać, korzystając z GenAI w celach służbowych?”  „W skrócie: o czym pamiętać korzystając z GenAI w celach służbowych” – informacje są dublowane. | Warto rozważyć umieszczenie sekcji „W skrócie: o czym pamiętać korzystając z GenAI w celach służbowych”oraz warto rozważyć przebudowę całego dokumentu, aby miał on formułę „Zasady bezpiecznego korzystania z GenAI”. | Uwzględniono |
|  | **MF** | Str. 9 | W sekcji „GenAI w chmurze bez dedykowanego dostępu” wielokrotnie powtórzono jakich danych nie wrzucać do promptu. |  | Uwzględniono |
|  | **MF** |  | Warto rozważyć wyłączenie sekcji technicznej do osobnego pełnego dokumentu. |  |  |
|  | **MF** | Str. 12 | W sekcji „System godny zaufania” warto rozważyć dodatkowy zapis dotyczący konieczności przeprowadzania analizy etycznych skutków dla każdej z implementacji z uwzględnieniem postanowień zawartych w opracowaniu, sporządzonym przez niezależną grupę ekspertów wysokiego szczebla ds. AI powołaną przez KE w czerwcu 2018, noszącym tytuł „Wytyczne w zakresie etyki dotyczące godnej zaufania sztucznej inteligencji” oraz zawartej w tymże opracowaniu ” Listy kontrolnej oceny godnej zaufania AI”. |  | Propozycje będą rozważane przy tworzeniu zbioru wytycznych dla Urzędów (w przygotowaniu). |
|  | **MF** | Str. 2 | „…narzędzi opartych o sztucznej inteligencji, które…” | Sugerujemy zamienić na „opartych na sztucznej inteligencji” | Nie uwzględniono |
|  | **MF** | Str. 2 | „Te narzędzia określa się jako tzw. generatywną sztuczną inteligencję (dalej: GenAI), którą to nazwę stosuje się zamiennie z określeniami takimi jak duże modele językowe (Large Language Models, LLM) | GenAI nie jest tożsame z LLM, które jest pojęciem węższym. GenAI może dotyczyć także generowania informacji z wykorzystaniem innych modeli, niekoniecznie LLM, które są stosowane głównie do generowania tekstów. | Uwzględniono |
|  | **MF** | Str. 2 | „Pojawienie się i upowszechnienie takich narzędzi z stwarza…” | Sugerujemy usunięcie „z”. | Uwzględniono |
|  | **MF** | Str. 2 | „Jego głównym celem, obok prezentacji tej technologii oraz jej użyteczności, wsparcie pracowników sektora publicznego w minimalizowaniu ryzyka niewłaściwego i potencjalnie szkodliwego wykorzystania GenAI.” | Wydaje się, że osiągnięcie wskazanego celu wymaga stworzenia zdecydowanie szerszego materiału, warto rozważyć doprecyzowanie celu dokumentu, np. „wstępne zapoznanie”, „podstawowe informacje”. | Uwzględniono |
|  | **MF** | Str. 2 | „Ostatnia część jest najbardziej techniczna i opisuje rekomendacje użycia GenAI zależnie od modelu dostępu oraz dalsze technologiczne rekomendacje, które warto wziąć pod uwagę przy wyborze systemów sztucznej inteligencji do użycia i zakupienia do urzędu.” | Z tego fragmenty wynika, że rekomendacje nie dotyczą tylko GenAI, ale wszystkich systemów AI, co jak się wydaje rozszerza perspektywę dokumentu. | Uwzględniono |
|  | **MF** | Str. 3 | „Generatywna … (ang. prompt)” | W dalszej części raportu zrezygnowano z takiego sposobu oznaczania i wprowadzania terminów obcojęzycznych, warto ujednolicić metodę w całym tekście. | Uwzględniono |
|  | **MF** | Str. 3 | „Algorytmy modeli generatywnej sztucznej inteligencji działają w oparciu o dostarczone na etapie tworzenia narzędzia dane w procesie nazywanym „trenowaniem” | Dane dostarczane są na każdym etapie życia systemu AI, nie tylko w momencie tworzenia narzędzia. | Uwzględniono |
|  | **MF** | Str. 3 | „W skrócie: o czym pamiętać korzystając z GenAI w celach służbowych” | W urzędach powinna zostać utworzona lista narzędzi opartych o GenAI, z których mogą w celach służbowych korzystać pracownicy, a każde kolejne narzędzie powinno być weryfikowane. Oczywiście każde wykorzystanie narzędzia powinno odbyć się z uwzględnieniem wskazanych rekomendacji dotyczących stosowania AI.  W tym fragmencie warto uwypuklić kwestię indywidualnego dopuszczenia stosowania genAI w celach służbowych przez dany resort. | Propozycje będą rozważane przy tworzeniu zbioru wytycznych dla Urzędów (w przygotowaniu). |
|  | **MF** | Str. 3 | „Nie należy wprowadzać do takich narzędzi informacji lub dokumentów, które” | Przed wypunktowaniem sugerujemy dodać „:” | Uwzględniono |
|  | **MF** | Str. 3 | „• są niejawne lub zawierają dane wrażliwe.  • zawierają informacje urzędowe będące w fazie przygotowawczej, a tym samym nie przeznaczone do upublicznienia;  • naruszają przepisy o ochronie danych osobowych.” | Sugerujemy ujednolicenie znaków interpunkcyjnych używanych po każdym kolejnym wypunktowaniu. | Uwzględniono |
|  | **MF** | Str. 4 | „GenAI to narzędzie z dużym potencjałem zastosowania, które przy zachowaniu należytej staranności może być pomocne w usprawnieniu realizowanych zadań.” | Warto doprecyzować co rozumie się w tym kontekście pod sformułowaniem należytej staranności oraz kto powinien ją zachować. | Nie uwzględniono |
|  | **MF** | Str. 12 | „Należy używać modeli na licencji typu open-source zamiast technologii zamkniętych.” | Warto rozważyć, czy pracownik merytoryczny (nie developer) będzie umiał to ocenić oraz czy nie stonować przekazu, z uwagi na fakt, że wybierane rozwiązania, w tym bazujące na GenAI powinno być optymalne pod wieloma względami, bez przeważającej wartości faktu czy rozwiązanie jest typu *open source*. | Propozycje będą rozważane przy tworzeniu zbioru wytycznych dla Urzędów (w przygotowaniu). |
|  | **MF** | Str. 12 | „Należy używać modeli typu glass-box zamiast modeli typu black-box” | Warto rozważyć czy pracownik merytoryczny (nie developer) będzie umiał to ocenić oraz zastosowanie powszechnie używanego w literaturze określenia *white-box* zamiast *glass-box*. | Propozycje będą rozważane przy tworzeniu zbioru wytycznych dla Urzędów (w przygotowaniu). |
|  | **MF** |  | Należy pamiętać, że jeśli chcemy korzystać z narzędzi automatycznego tłumaczenia tekstów lub dokumentów istnieją dedykowane takim funkcjom rozwiązania wykorzystujące AI, które nie są modelami i systemami generatywnymi | Rekomendacje powinny dotyczyć stosowania AI, a nie tylko jednej z jej dziedzin – GenAI. | Nie uwzględniono. Materiał jest wprowadzeniem do GenAI |
|  | **MF** |  | Warto rozważyć zdefiniowanie adresata części tekstu w każdej z części. |  | Adresatem materiału jest pracownik administracji publicznej, który nie miał wcześniej styczności z pojęciem GenAI |
|  | **MF** | Str. 12 | „Retrenowanie modelu powinno odbywać się tylko na uporządkowanych danych zweryfikowanych statystycznie.” | Wydaje się, że zagadnienie nie dotyczy bezpośrednio cyberbezpieczeństwa, tylko procesu modelowania. | Propozycje będą rozważane przy tworzeniu zbioru wytycznych dla Urzędów (w przygotowaniu). |
|  | **MF** | Str. 12 | „Domyślnie modele nie powinny być trenowane na danych osobowych.” | Wydaje się, że bez przedstawienia szerszego kontekstu powyższy punkt może być mylący/niejednoznaczny. | Propozycje będą rozważane przy tworzeniu zbioru wytycznych dla Urzędów (w przygotowaniu). |
|  | **PUODO** | „W skrócie: o czym pamiętać korzystając z GenAI w celach służbowych” | Projekt dokumentu w części „W skrócie: o czym pamiętać korzystając z GenAI w celach służbowych” opiera się na założeniu, że to użytkownik będzie odpowiadał za sposób oraz skutki wykorzystania narzędzi z zakresu sztucznej inteligencji. Dokument nie definiuje natomiast najważniejszej kwestii: czy będzie to pracownik czy pracodawca. | Wskazać należy, że odpowiedzialność za ocenę pozyskiwanych danych osobowych przez pracownika do celów służbowych powinna być przypisana pracodawcy jako administratorowi danych osobowych. Powinno to być wyraźnie określone w przedmiotowych rekomendacjach. Administrator odpowiada za zapewnienie poszanowania przepisów dotyczących przetwarzania danych osobowych, w tym ogólnego rozporządzenia o ochronie danych, i wynikających z nich zasad ochrony danych osobowych. Ma on obowiązek zastosowania środków technicznych i organizacyjnych zapewniających ochronę przetwarzanych danych odpowiednią do zagrożeń oraz kategorii danych objętych ochroną. W ocenie Prezesa UODO przyjęcie przez pracodawcę określonego narzędzia usprawniającego pracę (opartego na generatywnej sztucznej inteligencji) powinno zostać poprzedzone przeprowadzoną oceną skutków dla ochrony danych3 . Przeprowadzenie takiej analizy powinno prowadzić do wykazania niezbędności przetwarzania danych osobowych w określony sposób, we wskazanym konkretnie celu (celach) i zakresie oraz oceny ryzyka projektowanych (przyjmowanych) rozwiązań w zakresie przetwarzania danych osobowych. Projektowane założenia ze względu na zakładaną skalę, zakres i sposoby przetwarzania danych osobowych powodować mogę szeroki wachlarz ryzyk dla prywatności i danych osobowych. Do tej materii odnosi się motyw 91 rozporządzenia 2016/679 wskazujący w odniesieniu do operacji przetwarzania o dużej skali, że są to operacje, które „służą przetwarzaniu znacznej ilości danych osobowych na szczeblu regionalnym, krajowym lub ponadnarodowym i które mogą wpłynąć na dużą liczbę osób, których dane dotyczą, oraz które mogą powodować wysokie ryzyko, na przykład (ze względu na swój szczególny charakter) gdy zgodnie ze stanem wiedzy technicznej stosowana jest na dużą skalę nowa technologia – oraz do innych operacji przetwarzania powodujących wysokie ryzyko naruszenia praw lub wolności osób, których dane dotyczą, w szczególności gdy operacje te utrudniają osobom, których dane dotyczą, wykonywanie przysługujących im praw”. Przyjęte w dniu 4 kwietnia 2017 r. Wytyczne Grupy Roboczej Art. 29 dotyczące oceny skutków dla ochrony danych oraz pomagające ustalić, czy przetwarzanie „może powodować wysokie ryzyko” do celów rozporządzenia 2016/679 (WP248 rev.01) wskazują na konieczność wybrania metodyki dokonywania oceny skutków dla ochrony danych, która spełnia kryteria określone w załączniku 2 do wytycznych. Niezależnie od niezbędności dokonania oceny skutków dla ochrony danych tworzone rozwiązania muszą uwzględniać zasady przetwarzania danych osobowych wynikające z art. 5 RODO. Należy zwrócić uwagę na zakres danych, których nie należy wprowadzać do narzędzi AI (wzgląd na zasadę minimalizacji danych – art. 5 ust. 1 lit. c RODO). Z projektu wynika, że: „Nie należy wprowadzać do takich narzędzi informacji lub dokumentów, które: są niejawne lub zawierają dane wrażliwe; zawierają informacje urzędowe będące w fazie przygotowawczej, a tym samym nie przeznaczone do upublicznienia; naruszają przepisy o ochronie danych osobowych (strona 3 dokumentu). W tym miejscu należy zaakcentować ryzyka, jakie wiążą się z wykorzystywaniem danych osobowych w narzędziach AI w treściach tzw. krytycznych. Narzędzia AI usprawniające pracę powinny być wykorzystywane nie w generowaniu całych materiałów bez udziału nadzoru człowieka, lecz mogą stanowić uzupełnienie pracy ludzkiej. Powinny być wykorzystywane w obszarach „mniej twórczych”, gdzie ewentualne ryzyko nie będzie odczuwalne tak, jak w kluczowych projektach (np. zawierających duże bazy danych, w tym danych o charakterze osobowym). Wszelkie obszary pracy związane z wykorzystywaniem narzędzi AI powinny być uprzednio zidentyfikowane przez administratora i poddane szczególnej analizie, w tym pod kątem zakresu danych osobowych. Zwrócić uwagę należy, że narzędzia AI usprawniające pracę nie powinny być wykorzystywane w sprawach skomplikowanych, wymagających indywidualnego podejścia. Ich rola to przede wszystkim pomoc w sprawach rutynowych (np. związanych m.in. z automatyczną obsługą spraw w urzędach). Należy pamiętać, że narzędzie to nie jest nieomylne, bowiem opiera się przede wszystkim na prawdopodobieństwie, a generowane treści mogą zawierać błędy, co może wywoływać negatywne konsekwencje dla osoby, której dane są przetwarzane przez generatywną sztuczną inteligencję. W analizie zagrożeń dla ochrony danych przy ostatecznym wypracowywaniu przedmiotowego dokumentu na pewno pomocne będzie wsparcie specjalistów z zakresu ochrony danych jakimi są inspektorzy ochrony danych, których zadaniem jest m.in. monitoring i kontrola stosowanych u administratora procedur, oświadczeń woli, sposobu realizacji uprawnień podmiotów danych. Należy mieć na uwadze, że administratorzy są przede wszystkim związani przepisami obowiązującego prawa. Powstaje zatem pytanie czy oprócz opiniowanych rekomendacji planowane są prace legislacyjne w przedmiotowym zakresie. Jeśli tak, Prezes UODO deklaruje swoje wsparcie w tym zakresie. | Propozycje będą rozważane przy tworzeniu zbioru wytycznych dla Urzędów (w przygotowaniu). |
|  | **MRIT** | Uwaga ogólna | Autorzy poświęcili niewiele uwagi zagadnieniu uświadomienia użytkownika o potencjalnych trudnościach w usuwaniu wprowadzonych do GenAI informacji oraz o zależnościach dot. takiego usuwania wynikających z modelu wdrożenia GenAI tj. chmura vs. on-premise | Zaleca się uwzględnić w treści dokumentu, zagadnienie usuwania wprowadzonych do GenAI danych. | Nie uwzględniono.  Kwestie będą szczegółowo omówione w zbiorze wytycznych dla Urzędów (w przygotowaniu). |
|  | **MRiT** | Uwaga ogólna | W systemach EZD poszczególnych resortów znajdują się dziesiątki tysięcy dokumentów. Jest to punkt wyjściowy do budowy własnego, zamkniętego LLM dla polskiej administracji rządowej lub wykorzystania tworzonych obecnie w Polsce polskich LLM. Przy migracji systemów typu EZD do systemu EZD RP, i migracji z systemów poszczególnych resortów do modelu wspólnej chmury rządowej powstałaby okazja do wprowadzenia optymalizacji i ułatwień dla całej administracji lub budowy systemu generatywnej sztucznej inteligencji dla polskiej administracji rządowej począwszy jako dodatku do systemu EZD a skończywszy na kastomizowanym narzędziu typu Copilot. |  | To zagadnienie nie jest przedmiotem tego opracowania. |
|  | **MRiT** | Uwaga ogólna | Do rozważenia:  Na str. 4 zamiast sformułowania *„wskazane jest oznaczenie, które treści zostały przygotowane ze wsparciem sztucznej inteligencji*” proponujemy użyć *„wymagane jest oznaczenie, które treści zostały przygotowane ze wsparciem sztucznej inteligencji”.*  Ułatwi to późniejszą analizę pod kątem praw autorskich oraz ocenę efektywności wykorzystania GenAI. |  | Uwzględniono |
|  | **MRiT** | Uwaga ogólna | W dokumencie za mało uwagi poświęcono na to w jaki sposób zamawiać w administracji rozwiązania oparte o AI. | Dokument powinien zostać uzupełniony o wytyczne dotyczące zamawiania rozwiązań AI np.:   1. Na co zwrócić uwagę w szczególności w kontekście modelu dostępu i np. utrzymywania w chmurze (czy dane są przetwarzane np. w Europie) 2. Jak systemy powinny być opisane dla zewnętrznego użytkownika 3. Jakie wytyczne powinno się zawrzeć w umowach z dostawcami narzędzia 4. Jakie zasoby ludzkie powinny być wymagane od dostawcy, żeby właściwie trenować model i jak długo taki zasób powinien wspomagać Zamawiającego 5. Jak powinno się podchodzić do przygotowania takiego zamówienia w fazie pre-trenowania, jak przygotować dane i jakie zasoby powinno się po stronie Zamawiającego dedykować, aby nadzorować fazę przygotowania,   Jak opisać zasoby (niezbędne do tego, aby operacje i zapytania przetwarzane były szybko), czy tak jak system teleinformatyczny i usługi chmurowe | Nie uwzględniono.  Te kwestie będą szczegółowo omówione w zbiorze wytycznych dla Urzędów (w przygotowaniu). |
|  | **MRIT** | „W skrócie: o czym pamiętać korzystając z GenAI w celach służbowych” |  | Dopisać akapit: „**Utrudnione usuwanie danych”** i uzupełnić o treść „Wprowadzając informację np. zapytania do GenAI należy czynić to z rozwagą, mając na względzie, że ich późniejsze usunięcie może być bardzo trudne lub wręcz niemożliwe do usunięcia.” | Uwzględniono |
|  | **MRIT** | „O czym należy pamiętać, gdy wchodzi się w interakcję z GenAI - zwłaszcza w celach służbowych?” | Pomimo, iż kierunkowo treść dokumentu jest sformułowana prawidłowo jednak dla użytkownika nie musi być oczywistym fakt, że GenAI w chmurze publicznej nie zapomina niczego oraz że w przypadku wprowadzenia nadmiarowych danych lub danych naruszających przepisy ich usunięcie może być niemożliwe. | Proponuje się dopisać dodatkowo (na czerwono) jedno zdanie pod listą zapisaną na czerwono o przykładowym brzemieniu: „Należy pamiętać, że informacje raz wprowadzone do systemu GenAI, mogą być niemożliwe do późniejszego usunięcia”  Poniżej zdania „Zasady te mogą być mniej restrykcyjne w odniesieniu do dokumentów urzędowych jeśli GenAI jest częścią architektury informatycznej urzędu i objęty systemem cyberbezpieczeństwa instytucji. ” zaleca się dopisać zdanie o przykładowym brzemieniu: „W trakcie wyboru rozwiązania GenAI umiejscowionego w infrastrukturze urzędu należy uwzględnić kwestie możliwości skutecznego usuwania danych wynikowych bazujących na wprowadzonych do systemu informacjach, usuwaniu wprowadzanych informacji oraz zapewniających możliwość całkowitego lub częściowego usuwania wprowadzanych danych źródłowych(zasilających model GenAI)” | Uwzględniono  Te kwestie będą szczegółowo omówione w zbiorze wytycznych dla Urzędów (w przygotowaniu) |
|  | **MRIT** | „GenAI w chmurze bez dedykowanego dostępu” | Brak zapisu o nieusuwalności informacji w chmurze publicznej | Zaleca się dopisać na końcu rozdziału zdanie o przykładowym brzemieniu: „Należy zwrócić szczególną uwagę na wprowadzane do publicznego/chmurowego modelu GenAI, gdyż ich późniejsze usunięcie może być niemożliwe” | Nie uwzględniono. Te kwestie będą szczegółowo omówione w zbiorze wytycznych dla Urzędów (w przygotowaniu) |
|  | **MRIT** | „Jaki wybrać i przygotować system?”  Podrozdział: „Bezpieczeństwo i przejrzystość” | Brak zapisu o nieusuwalności informacji w modelu GenAI | Zaleca się dopisać w punkcie 1. podpunkt f) o przykładowym brzmieniu: „zapewnienie możliwości usuwania informacji wprowadzonych poprzez zasilenie źródłowe treścią jak i informacji wprowadzonej poprzez interfejs użytkownika” | Nie uwzględniono. Te kwestie będą szczegółowo omówione w zbiorze wytycznych dla Urzędów (w przygotowaniu) |
|  | **MRIT** | „Jaki wybrać i przygotować system?”  Podrozdział: „Cyberbezpieczeństwo” | Nieuwzględnienie zagadnienia związanego z integracją z systemami zewnętrznymi AI (dotyczy systemów instalowanych w urzędach).  W sytuacji takiej integracji powstaje niepewność jakie dane są wysyłane/odbierane z chmury i czy takie rozwiązanie jest dopuszczalne w rozumieniu cyberbezpieczeństwa. | Dopisać poniżej punktu 4, zdanie o przykładowym brzmieniu: „W przypadku gdy system został zainstalowany w modelu „on-premise” (w urzędzie) należy zwrócić uwagę czy i w jakim stopniu nie pozostaje on zintegrowany z zewnętrznymi systemami AI i czy taka integracja jest konieczna” | Nie uwzględniono.  Te kwestie będą szczegółowo omówione w zbiorze wytycznych dla Urzędów (w przygotowaniu) |