PREZES
URZĘDU OCHRONY
DANYCH OSOBOWYCH
Mirosław Wróblewski

Warszawa, *17-07-2025*

DPNT.071.26.2025

Pan
Dariusz Standerski
Sekretarz Stanu
w Ministerstwie Cyfryzacji

Szanowny Panie Ministrze,

w związku ze skierowaniem do publicznych konsultacji **„Polityki rozwoju sztucznej inteligencji w Polsce do 2030 roku”** (dalej jako: „Polityka AI”) **Prezes Urzędu Ochrony Danych Osobowych** – realizując zadania nadane mu jako organowi właściwemu w sprawie ochrony danych osobowych przez art. 57 ust. 1 lit. c rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679[1](dalej jako: rozporządzenie 2019/679) – niniejszym pismem zgłasza uwagi do ww. dokumentu. Uwagi te wypracowane zostały po odbyciu wewnętrznej debaty ekspertów UODO z członkami grupy roboczej ds. sztucznej inteligencji Społecznego Zespołu Ekspertów przy Prezesie UODO oraz ze Społecznym Zespołem Ekspertów przy Prezesie UODO.

I. Uwagi ogólne i dotyczące struktury dokumentu

Opublikowana Polityka AI prezentuje zaktualizowane i rozbudowane cele oraz działania w ślad za sformułowaną w „Strategii Cyfryzacji Państwa do 2035 r.” wizją, zgodnie z którą rozwój sztucznej inteligencji to jeden z kluczowych obszarów w zakresie

[1] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz. Urz. UE L 119 z 4.5.2016, str. 1 ze zm.).

transformacji cyfrowej Polski. Rozwój sztucznej inteligencji jest warunkiem koniecznym utrzymania, a nawet zdynamizowania tempa wzrostu gospodarczego w Polsce, zwiększenia konkurencyjności krajowej gospodarki oraz wzrostu efektywności działania administracji publicznej. Podjęcie zatem inicjatywy w sprawie opracowania Polityki AI i przedstawienie jej do szerokich konsultacji należy zatem ocenić bardzo pozytywnie.

Równocześnie jednak Polityka AI powinna odpowiadać na powodowane przez sztuczną inteligencję wyzwania dla bezpieczeństwa we wszystkich jego aspektach – od bezpieczeństwa obywatela i jego danych, aż po bezpieczeństwo narodowe. Powinna uwzględniać również kwestię interoperacyjności – powiązania chociażby ze strategią „AI Continent"[2] czy zobowiązaniami wynikającymi z Konwencji 108+ Rady Europy.

Wymagane (i nieobecne w Polityce AI) podejście do aspektów bezpieczeństwa danych osobowych, poza ogólnym, horyzontalnym odniesieniem do zgodności z regulacją dotyczącą ochrony danych osobowych wydaje się być niewystarczające i nie powinno mieć charakteru odrębnego od pozostałych celów, kluczowych wskaźników efektywności (tzw. KPI – *Key Performance Indicators*) i zakładanych działań, ale powinno stanowić immanentną część składową każdego z zarysowanych w Polityce AI bloków tematycznych. Zapewnienie bowiem wymaganego poziomu bezpieczeństwa i zagwarantowanie standardów ochrony danych osobowych powinno być naturalnym i wymaganym ogniwem łańcucha wartości każdego z procesów tworzących zdefiniowane w Polityce bloki tematyczne.

Tymczasem mieszany charakter dokumentu, łączący zarówno cechy polityki (normatywnej), jak i bardziej szczegółowej strategii (operacyjnej) powoduje trudności w przełożeniu ogólnych założeń na konkretne, mierzalne wskaźniki, cele lub warunki ich osiągnięcia, zwłaszcza te najistotniejsze z punktu widzenia obszaru właściwości organu do spraw ochrony danych osobowych, a więc realizowane z perspektywy zapewnienia gwarancji dla skutecznej realizacji prawa do ochrony danych osobowych.

Z tych względów istotna byłaby zmiana konstrukcji dokumentu i odejście od podejścia silosowego – przedmiotowego, do sektorowego. Pozwoliłoby to, przy określeniu całościowego celu polityki, na wskazanie obszarów (sektorów), w których przewidywane ma być działanie stanowiące element osiągnięcia celu ogólnego. To z kolei umożliwi określenie warunków, które muszą być spełnione w poszczególnych obszarach aktywności państwa, także z perspektywy gwarancji dla prawa do ochrony danych osobowych i prawa do prywatności.

Warunki określające środki i zasady ochrony danych (w tym w aspekcie regulacyjnym, otwartości danych, itp.) są ściśle kontekstowe i różne w poszczególnych sektorach. Formułowanie zatem warunków w oderwaniu od sektorów (życia, gospodarki, prawa), zwłaszcza w obszarze bezpieczeństwa i ochrony danych osobowych ma zbyt niski walor informacyjny i nie pozwala na prawidłowe ich określenie. Zaprezentowane w Polityce AI podejście powoduje niewystarczające uwzględnienie prawa do ochrony danych osobowych w kluczowych jej obszarach.

Obecna struktura dokumentu sprawia, że nie do końca jasno wskazane zostały konkretne cele zarówno w poszczególnych podrozdziałach, jak też w kontekście całego

[2] https://digital-strategy.ec.europa.eu/en/library/ai-continent-action-plan

dokumentu. Organ właściwy w sprawie ochrony danych osobowych proponuje rozważenie opracowania jednolitej struktury Polityki AI, w której cele oraz KPI umieszczane byłyby na końcu każdej sekcji i bezpośrednio zestawiane z odpowiadającymi im działaniami. To pozwoliłoby na łatwe zestawienie celów z mierzalnymi wskaźnikami, które do nich się odnoszą.

Cenne byłoby również odniesienie w każdej sekcji dokumentu do zagadnień związanych z bezpieczeństwem/cyberbezpieczeństwem rozwiązań AI oraz danych wykorzystywanych do trenowania i wnioskowania, zwłaszcza w kontekście przetwarzania danych objętych szczególnymi reżimami przetwarzania, danych szczególnych kategorii. „Dane jako paliwo" dla rozwiązań sztucznej inteligencji są kluczowym zasobem i należy bardzo dobitnie podkreślać aspekty bezpieczeństwa w tym obszarze. W kontekście zapewnienia suwerenności technologicznej Polski istotne byłoby przyjęcie podejścia polegającego na klasyfikacji danych od krytycznych dla bezpieczeństwa kraju i obywateli do najmniej krytycznych i wokół takiej klasyfikacji wskazywać metody, zasady oraz miejsca przetwarzania takich zasobów.

II. Uwagi szczegółowe w aspekcie ochrony danych osobowych

Pomimo, że organ właściwy w sprawie ochrony danych osobowych przestawił swoje stanowisko względem koncepcji rozwoju cyfryzacji Polski zawartej w „Strategii Cyfryzacji Państwa do 2035 r.", w tym sztucznej inteligencji[3], to również planowane Polityką AI podjęcie działań, by projektowanie, opracowywanie, wdrażanie i wykorzystywanie rozwiązań sztucznej inteligencji odbywało się z poszanowaniem praw podstawowych (nie tylko prawa do prywatności, ale także prawa do ochrony danych osobowych – wszak zarówno na gruncie Karty praw podstawowych UE, jak i Konstytucji RP są to dobra odrębnie chronione) wymaga uwzględnienia na szczeblu krajowym europejskiego kontekstu regulacyjnego w zakresie m.in. przepisów dotyczących ochrony i bezpieczeństwa danych osobowych.

W założeniach Polityki AI nie została uwzględniona w dostatecznym stopniu materia ochrony danych osobowych, a aspekty jej dotyczące zostały przedstawione na dużym poziomie ogólności – dlatego też organ właściwy w sprawie ochrony danych osobowych kieruje poniżej sformułowane postulaty związane z kwestią ochrony danych osobowych, które powinny również zostać odzwierciedlone w dokumencie strategicznym dla koncepcji rozwoju sztucznej inteligencji w Polsce.

1. Podstawy prawne przetwarzania danych osobowych w poszczególnych sektorach.

Jednym ze zidentyfikowanych wyzwań w obszarze rozwoju AI w społeczeństwie, jako **sztucznej inteligencji godnej zaufania** jest „wdrożenie przepisów unijnych i stworzenie krajowych ram regulacyjnych w sposób przyjazny dla biznesu oraz chroniący prawa obywateli i konsumentów". Zakres przedstawionych działań w tym względzie na

[3] Pismem z 12 grudnia 2024 o sygn. DOL.401.502.2024.

potrzeby **„Regulacji prawnych i etyki AI”** nie zawiera jednak kierunkowego odniesienia się ani planu działania państwa w tym obszarze (a tym bardziej konkretnych rozwiązań).

W konsekwencji istotne byłoby **uszczegółowienie planu tworzenia ram prawnych** dla rozwoju sztucznej inteligencji w Polsce **z uwzględnieniem unijnego systemu regulacyjnego, zarówno na płaszczyźnie horyzontalnej, jak i sektorowej**.

Również realizacja jednego z celów zakładanych w Polityce AI, tj.: **„Sprawne Państwo wykorzystujące rozwiązania sztucznej inteligencji”** powinna uwzględniać zagwarantowanie **podstaw prawnych dla działań podejmowanych przez organy publiczne** czy **podmioty realizujące zadania publiczne** (zarówno na poziomie centralnym, jak i samorządowym) z wykorzystaniem narzędzi sztucznej inteligencji.

Dlatego też wdrażanie sztucznej inteligencji w poszczególnych obszarach funkcjonowania państwa oraz działach administracji publicznej wymaga w pierwszej kolejności **przeglądu obowiązujących przepisów** i **ustanowienia właściwych podstaw prawych** zgodnie z konstytucyjną zasadą praworządności oraz z poszanowaniem praw jednostki w procesie stanowienia prawa i zapewnieniem gwarancji zawartych w Karcie praw podstawowych UE (art. 7 - poszanowanie życia prywatnego, ale i art. 8 – ochrona danych osobowych), regulacji odnoszących się wyłącznie do przetwarzania danych w konkretnych aspektach spraw karnych, tj. dyrektywie 2016/680 oraz rozporządzeniu 2016/679, w szczególności z uwzględnieniem warunków wskazanych w art. 6 ust. 3 tego aktu, dla wykonania zadania realizowanego w interesie publicznym (art. 6 ust. 1 lit c) lub w ramach sprawowania władzy publicznej powierzonej administratorowi (art. 6 ust. 1 lit e). W przypadku przetwarzania danych szczególnych kategorii czy danych dotyczących karalności konieczne jest ponadto zadośćuczynienie dyspozycjom art. 9 ust. 2 warunkującym dopuszczalność odstąpienia od zakazu przetwarzania takich danych (art. 9 ust. 1) oraz art. 10 rozporządzenia 2016/679, poprzez zastosowanie dodatkowych zabezpieczeń i środków ochrony praw podstawowych, wolności i interesów podmiotów danych.

Rozważenia wymaga także weryfikacja zasadności ingerencji ustawowej w celu określenia podstaw prawnych przede wszystkim dla trenowania modeli AI z perspektywy ustalenia zgodności innego celu, w którym dane są już przetwarzane, z celem, w którym dane zostały zebrane w oparciu o reguły określone w art. 6 ust. 4 i art. 23 rozporządzenia 2016/679. Taka analiza będzie prowadziła do możliwie różnych wniosków w różnych sektorach, zarówno z perspektywy prawa do ochrony danych, prawa do prywatności, jak i interesów państwa.

Zapewnienie w przepisach prawa rangi ustawy transparentności działania systemów sztucznej inteligencji, przejrzystości i rzetelności co do wykorzystywania informacji / danych, w tym danych osobowych w ogólności jako zasilających te systemy, ale i danych będących wynikiem działania SSI pozwoli na zminimalizowanie ryzyk, nieprawidłowości lub nadużyć związanych z ich stosowaniem.

Z punktu widzenia ochrony praw podmiotów danych kwestią kluczową jest uregulowanie materii zautomatyzowanego podejmowania decyzji i profilowania z wykorzystaniem sztucznej inteligencji, zwłaszcza w odniesieniu do podmiotów sektora publicznego, realizujących zadania publiczne i obowiązanych do działania na podstawie i w granicach prawa, szczególnie zatem w kontekście podstaw prawnych dotyczących

tego rodzaju operacji przetwarzania, ważenia dóbr chronionych i interesów państwa przy tworzeniu regulacji powszechnie obowiązujących, udzielania zgody, spełniania obowiązku informacyjnego, realizowania prawa do interwencji ludzkiej, czy wdrażania właściwych środków ochrony interesów osób, których dane dotyczą.

Zatem stosowanie systemów sztucznej inteligencji przez podmioty sektora publicznego czy dla realizacji zadań publicznych wymaga przyjęcia przejrzyście skonstruowanych **przepisów sektorowych, jak i ustaw regulujących funkcjonowanie poszczególnych podmiotów (organów). Stanowienie przepisów regulujących zasady i sposoby, ale przede wszystkim cele funkcjonowania systemów sztucznej inteligencji i przyjęte środki ochrony** powinno być poprzedzone przeprowadzeniem oceny skutków w zakresie praw podstawowych zgodnie z art. 27 aktu w sprawie sztucznej inteligencji (AI Act)[4] oraz stosowną analizą odpowiednio do ratio legis warunków z art. 6 ust. 3 oraz art. 9 ust. 2-4 rozporządzenia 2016/679. Być może właściwym rozwiązaniem byłaby regulacja na kształt ustawy zapewniającej stosowanie rozporządzenie 2016/679[5], czyli ustawa wprowadzająca rozwiązania w poszczególnych sektorach stosujących/wykorzystujących systemy AI.

Wnikliwego przeglądu obecnie obowiązujących przepisów polskich wymaga wykorzystywanie **rozwiązań sztucznej inteligencji w usługach publicznych obejmujących tak newralgiczne obszary, jak: ochrona zdrowia i wymiar sprawiedliwości, ale i w kontekście kategorii danych jakie miałyby być przetwarzane – zwłaszcza danych biometrycznych, dotyczących zdrowia, genetycznych, o karalności.**

Konieczne jest także dokonanie przeglądu regulacji krajowych – np. ustawy z dnia 6 listopada 2008 r. o prawach pacjenta i Rzeczniku Praw Pacjenta, ustawy z dnia 28 kwietnia 2011 r. o systemie informacji w ochronie zdrowia, czy ustawy z dnia 27 sierpnia 2004 r. o świadczeniach opieki zdrowotnej finansowanych ze środków publicznych - pod kątem ich dostosowania do reguł prawa dostępu do danych i zasad ich wykorzystywania wynikających z rozporządzenia EHDS[6], zwłaszcza co do wtórnego wykorzystywania danych.

Podobnie automatyzacja procesów stosowanych przez podmioty szeroko rozumianego wymiaru sprawiedliwości powinna być poprzedzona analizą obowiązujących regulacji w tym zakresie, by wdrożenie rozwiązań sztucznej inteligencji poprzedzone zostało ważeniem wartości jednostek i interesów ogólnych, interesów państwa oraz oparte zostało na warunkach określonych w przepisach rangi ustawowej

---

[4] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2024/1689 z dnia 13 czerwca 2024 r. w sprawie ustanowienia zharmonizowanych przepisów dotyczących sztucznej inteligencji oraz zmiany rozporządzeń (WE) nr 300/2008, (UE) nr 167/2013, (UE) nr 168/2013, (UE) 2018/858, (UE) 2018/1139 i (UE) 2019/2144 oraz dyrektyw 2014/90/UE, (UE) 2016/797 i (UE) 2020/1828 (akt w sprawie sztucznej inteligencji)Tekst mający znaczenie dla EOG (Dz. U. UE. L. z 2024 r. poz. 1689).

[5] Ustawa z dnia 21 lutego 2019 r. o zmianie niektórych ustaw w związku z zapewnieniem stosowania rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych)

[6] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2025/327 z dnia 11 lutego 2025 r. w sprawie europejskiej przestrzeni danych dotyczących zdrowia oraz zmiany dyrektywy 2011/24/UE i rozporządzenia (UE) 2024/2847 (Dz. U. UE. L. z 2025 r. poz. 327).

również z perspektywy rozwiązań zawartych w dyrektywie 2016/680[7] w związku z przetwarzaniem danych osobowych przez właściwe organy do celów zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania i ścigania czynów zabronionych i wykonywania kar, w tym ochrony przed zagrożeniami dla bezpieczeństwa publicznego i zapobiegania takim zagrożeniom.

Za ważną z punktu widzenia zaangażowania państwa na rzecz przejrzystości i odpowiedzialnego zarządzania sztuczną inteligencją należy uznać natomiast wskazaną w dokumencie **inicjatywę stworzenia jednolitej, dostępnej publicznie listy systemów AI używanych w administracji publicznej** wraz z opisem funkcji oraz podstawowych parametrów technicznych dostępnych dla obywateli w celu zwiększenia transparentności działań administracji publicznej, co jest istotne m.in. z perspektywy prawa dostępu do informacji gwarantowanej przez art. 61 Konstytucji RP oraz art. 11 Karty praw podstawowych UE, jak i prawa do dobrej administracji gwarantowanego przez art. 41 tej Karty.

Jednak, aby zakładana funkcja takiego rejestru/listy została spełniona upublicznione powinny zostać nie tylko **główne cechy** systemu sztucznej inteligencji, ale także cel jego funkcjonowania, podejmowane z jego użyciem **działania i skutki** tych działań.

2. Rola Prezesa Urzędu Ochrony Danych Osobowych jako organu właściwego w sprawie ochrony danych osobowych

Zgodnie z informacją zawartą w Polityce AI realizację celu jakim jest **„Gwarancja prawa do prywatności i ochrona danych osobowych”** ma umożliwić m.in. „udział Urzędu Ochrony Danych Osobowych w powstałym w oparciu o AI Act systemie nadzoru nad rynkiem systemów i modeli AI”, a „obecnie trwają prace nad ustanowieniem systemu nadzoru systemu AI (PUODO, KRIBSI), który w spójny sposób nadzorował będzie różne aspekty zgodnego z prawem i bezpiecznego przetwarzania danych osobowych dla AI”.

Dotychczas nie zostały w sposób niebudzący wątpliwości ustalone zasady sprawowania ww. nadzoru, ani nie zostały precyzyjnie określone mechanizmy współpracy oraz podziału kompetencji między Komisją Rozwoju i Bezpieczeństwa Sztucznej Inteligencji (KRIBSI) a Prezesem UODO (trwa proces legislacyjny dotyczący projektu ustawy o systemach sztucznej inteligencji).

Kluczową rolę organu właściwego w sprawie ochrony danych osobowych z perspektywy realizacji zasady godnej zaufania AI odgrywa jego niezależność zagwarantowana mocą art. 51 rozporządzenia 2016/679, do której odnosi się również motyw 10 AI Act. Istnieje ryzyko, że w projektowanej strukturze nadzoru nad SSI rola Prezesa UODO, jako niezależnego organu nadzorczego ustanowionego na mocy rozporządzenia 2016/679, nie zostanie w wystarczający sposób zagwarantowana, co

[7] Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/680 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych przez właściwe organy do celów zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania i ścigania czynów zabronionych i wykonywania kar, w sprawie swobodnego przepływu takich danych oraz uchylająca decyzję ramową Rady 2008/977/WSiSW (Dz. U. UE. L. z 2016 r. Nr 119, str. 89 z późn. zm.).

wywołuje ryzyko nie zapewnienia odpowiedniego standardu instytucjonalnej ochrony prawa do ochrony danych osobowych.

W szczególności bez jasnego rozgraniczenia kompetencji między organem nadzorującym AI Act a Prezesem UODO może dojść do zbędnych sporów kompetencyjnych. Stwarza to równocześnie ryzyko powstawania luk prawnych, wydawania sprzecznych wytycznych oraz niepewności prawnej dla przedsiębiorców, którzy będą musieli stosować się do wymogów obu łącznie stosowanych aktów prawnych.

W Polityce AI nie została wskazana kluczowa, prewencyjna rola Prezesa UODO w procesie projektowania systemów i regulacji (zgodnie z zasadą *privacy by design*). Dokument nie wskazuje na obowiązek konsultowania z Prezesem UODO na wczesnym etapie takich projektów, jak tworzenie publicznych zbiorów danych wrażliwych w ochronie zdrowia czy wymiarze sprawiedliwości. Może to prowadzić do sytuacji, w której ochrona danych będzie traktowana jako wymóg formalny do spełnienia na końcu procesu, a nie jego integralny jego element.

W Polityce AI zabrakło także planów wzmocnienia potencjału Urzędu Ochrony Danych Osobowych. Wdrożenie polityki AI na tak szeroką skalę, zwłaszcza w administracji publicznej, wygeneruje potrzebę stałego i wysoce specjalistycznego nadzoru nad skomplikowanymi systemami przetwarzającymi dane osobowe. Dokument nie wspomina o konieczności wzmocnienia kadrowego, technologicznego i finansowego Urzędu Ochrony Danych Osobowych, aby mógł on skutecznie sprostać nowym, złożonym wyzwaniom związanym z audytem i kontrolą algorytmów AI.

3. Różnice pomiędzy otwartymi danymi a zasadami rozporządzenia 2016/679

Przeglądowi – w kontekście działania systemów sztucznej inteligencji – powinny zostać poddane także obowiązujące regulacje w przedmiocie zasad otwartości danych, zasad i trybu udostępniania i przekazywania informacji sektora publicznego w celu ponownego wykorzystywania oraz podmiotów, które udostępniają lub przekazują te informacje.

W Polityce AI brakuje wyraźnego uwypuklenia relacji pomiędzy otwartością danych publicznych i ochroną danych osobowych, zwłaszcza w kontekście trenowania modeli AI. Uwzględnienie dotychczasowych regulacji i opracowań z tego obszaru umożliwiłoby ocenę konieczności i ewentualne zaprojektowanie niezbędnej aktywności czy to regulatora czy też ustawodawcy w danym sektorze. Konieczny jest zatem przegląd regulacji odnoszących się do otwartości danych, klasyfikacja danych według poziomu krytyczności oraz określenie zasad lub sposobu określenia zasad anonimizacji danych przed udostępnieniem, uwzględniając rosnącą moc rozliczeniową i wnioski z danych interferowanych. Jest to także niezwykle istotne w obszarze wtórnego wykorzystywania danych przewidzianego w EHDS, aktu, który przewiduje nie tylko nowe prawa związane z pierwotnym przetwarzaniem danych dotyczących zdrowia, ale także przynosi nową perspektywę – wspólną unijną przestrzeń danych w tak istotnym obszarze, jakim jest wykorzystanie i wymiana elektronicznych danych medycznych w całej Unii Europejskiej.

4. Mechanizmy zgodności z rozporządzeniem 2016/679 i AI Act

W Polityce AI brakuje mechanizmów zapewniających zgodność z przepisami o ochronie danych oraz AI Act. Dokument nie określa roli Prezesa UODO w ocenie projektów AI, ani obowiązków administratorów danych w tym zakresie.

5. Brak odniesienia do wymogu „*data protection by design and by default*"

Polityka AI pomija obowiązek uwzględniania ochrony danych w fazie projektowania i jako domyślnej ochrony danych (art. 25 rozporządzenia 2016/679). Wdrożenie AI bez analizy z perspektywy zasad przetwarzania, zwłaszcza zasady minimalizacji danych, w tym podkreślenia roli wymogu uwzględniania ochrony danych w fazie projektowania i oceny skutków dla ochrony danych, które są podstawowymi wymogami rozporządzenia 2016/679, może prowadzić do istotnego naruszenia praw jednostki.

6. Poziom opisu wymagań meta – brak korelacji z celami, planami i KPI

Polityka AI nie zawiera przełożenia ogólnych założeń na konkretne mierzalne wskaźniki. Nie zaproponowano KPI w zakresie prawa do ochrony danych, prawa do prywatności czy bezpieczeństwa informacji / cyberbezpieczeństwa rozumianego jako dobro państwa przekładające się na dobro jednostek czy grup społecznych.

Zasadnym wydaje się poddanie gruntownej rewizji zaproponowanych w Polityce KPI-ów. Szereg z nich ma charakter działań, formalnych zdarzeń lub też nazbyt ogólnie sformułowanych mierników. KPI zaś powinny precyzyjnie oddawać stany pożądane proponowanych w Polityce przedsięwzięć. Przykładowo: na s. 26 zawarto KPI: „Liczba uruchomionych programów zatrzymujących talenty (np. AI Talent Visa)" – ten postulat obejmuje raczej sposób postępowania (działanie), a nie oczekiwany stan, tj. określoną liczbę utrzymanych w Polsce specjalistów AI w danej jednostce czasu. Liczba uruchamianych programów w żaden sposób nie jest bowiem miernikiem skuteczności podejmowanych działań – jest tylko lapidarnym opisem tychże działań. Na s. 26 zawarto KPI: „Rozpoczęcie działalności przez Instytut IDEAS" – to postulat o charakterze formalnym, nie wnoszącym realnej i konkretnej wartości w pomiarze efektywności Polityki. Nie fakt rozpoczęcia działalności przez Instytut IDEAS świadczy bowiem o rzeczonej efektywności, ale oczekiwane (i zwymiarowane) efekty tejże działalności, których w Polityce nie przedstawiono. Powyższe dwa przykłady nieprawidłowo sformułowanych KPI-ów stanowią wyłącznie egzemplifikację systemowej niedoskonałości zaproponowanych w Polityce KPI-ów nie tylko w przytaczanym obszarze „Polskie ekosystem AI", ale i w pozostałych obszarach.

7. Brak wizji zagospodarowania infrastruktury, danych i talentów w interesie publicznym. Działania edukacyjne.

Dokument nie wyjaśnia, jak dostęp do zasobów infrastrukturalnych i danych ma służyć realizacji wartości demokratycznych oraz ochronie praw jednostki.

Warto byłoby również rozważyć rozszerzenie Polityki o działania ukierunkowane na edukację dorosłych w zakresie AI, w tym w zakresie ochrony danych osobowych, w kontekście budowania niezbędnych kompetencji do utrzymania się na rynku pracy. Kluczowy wydaje się również obszar zaangażowania polskich organizacji pracodawców, instytucji rynku pracy, partnerów społecznych oraz instytucji naukowych w celu opracowywania wytycznych dla tego typu działań. Kształcenie obywateli i wyposażanie ich w wiedzę w sposób transparentny, niezależny od działań prowadzonych przez wielkie firmy technologiczne, pozwoli im potem świadomie dobierać technologię do swoich potrzeb. Takie działania będą wspierać polskich dostawców technologii zwiększać ich konkurencyjność oraz wzmacniać suwerenność technologiczną kraju. Takie działania pozwolą również na świadome wykorzystywanie danych z analizą ryzyk i odpowiednim poziomem bezpieczeństwa, szczególnie w kontekście danych wrażliwych.

8. Niedostosowana struktura dokumentu do określenia wymagań i KPI

W Polityce AI brakuje jednoznacznego przypisania działań do celów i rezultatów. Wskaźniki są wybiórcze i nieskoordynowane. Potrzebna jest klarowna matryca cel – działania – KPI w obszarze ochrony danych, prywatności i bezpieczeństwa / cyberbezpieczeństwa.

9. Etyczne wykorzystanie technologii

Docenić należy, że w dokumencie odniesiono się do zagadnień dotyczących etycznego wykorzystania technologii. Jednak pojęcie “etycznego AI” powinno być zdecydowanie bardziej doprecyzowane, także w kontekście wykorzystania danych, profili interesariuszy. W aktualnym tekście Polityki AI część społeczno-humanistyczna potraktowana jest hasłowo, bez konkretnych celów i propozycji kluczowych działań.

10. Negatywne skutki AI

Rozbudowania i wzmocnienia wymaga aspekt negatywnych skutków AI zawarty w punkcie 6.1 Polityki AI poprzez wskazanie centralnych środków łagodzących negatywne oddziaływanie AI, szczególnie w kontekście ochrony danych, w tym wrażliwych i prywatności, ale także szerzej – dezinformacji, dyskryminacji i uprzedzeń (bias), profilowania, wpływu na środowisko czy wreszcie kwestii związanych z uzależnieniem od dużych firm (vs suwerenność technologiczna).

11. Bezpieczna identyfikacja elektroniczna osób fizycznych

W Polityce AI pominięto ponadto istotne – w kontekście zagrożeń generowanych przez AI i wzmacnianych przez technologie kwantowe – zagadnienie bezpiecznej identyfikacji elektronicznej obywateli, zapewniających realizację procesu identyfikacji elektronicznej, uwierzytelniania i autoryzacji z należytym poziomem bezpieczeństwa, tj. z wykorzystaniem środków identyfikacji elektronicznej na poziomie bezpieczeństwa: wysokim, w rozumieniu rozporządzenia eIDAS 2.0.

III. Wnioski

Analiza Polityki AI w aspekcie ochrony danych osobowych prowadzi do sformułowania następujących rekomendacji:

1. Uznanie ochrony danych osobowych za zasadę horyzontalną

- wprowadzenie zasad ochrony danych osobowych jako przekrojowego fundamentu całej Polityki AI, powiązanego z art. 8 Karty praw podstawowych UE i art. 51 Konstytucji RP,
- przyjęcie wyważonych ram regulacyjnych z jednej strony legalizujących działania organów publicznych stosujących rozwiązania sztucznej inteligencji, z drugiej budujących zaufanie obywateli (jednostek i grup społecznych) i przedsiębiorców do procesów opartych na AI, gwarantujących ich wyjaśnialność, przejrzystość i bezpieczeństwo, jak również z zachowaniem zasad dostępu do danych i ich wtórnego wykorzystywania (otwartości danych),
- włączenie prawa do ochrony danych osobowych (nie tylko prawa do prywatności rozumianego ogólnie) do każdego sektora Polityki AI: infrastruktury, zdrowia, edukacji, administracji publicznej, innowacji czy otwartych danych.

2. Uzupełnienie Polityki AI o obowiązki zgodności z rozporządzeniem 2016/679, AI Act i Konwencją 108+

- uzupełnienie Polityki AI o odniesienia do art. 25 i 35 rozporządzenia 2016/679 (uwzględnianie ochrony danych w fazie projektowania oraz domyślna ochrona danych oraz ocena skutków), a w konsekwencji oszacowanie ryzyka naruszeń praw lub wolności osób fizycznych,
- wskazanie mechanizmów zgodności z AI Act oraz roli Prezesa UODO jako niezależnego organu nadzorczego,
- odniesienie do ram prawnych Rady Europy, w szczególności Konwencji 108+.

3. Rewizja systemu nadzoru – zapewnienie roli Prezesa UODO

- wprowadzenie jasnych mechanizmów współpracy między Komisją Rozwoju i Bezpieczeństwa SI (KRIBSI) a Prezesem UODO,
- uwzględnienie roli konsultacyjnej i prewencyjnej UODO (a nie wyłącznie nadzorczej ex post),
- przewidzenie wzmocnienia kadrowego i technologicznego UODO w celu wykonywania audytów i nadzoru nad wdrażaniem systemów AI.

4. Przekształcenie struktury dokumentu i KPI

- zapewnienie spójności strukturalnej dokumentu – rozdziały powinny być ujęte sektorowo i zawierać: cele, skorelowane z celem ogólnym → działania → warunki realizacji → KPI,
- KPI powinny być realistyczne, mierzalne i powiązane z efektami (nie tylko formalnymi zdarzeniami),

- wprowadzenie wskaźników odnoszących się do ochrony danych, transparentności i audytowalności.

5. Uwzględnienie ryzyk związanych z otwartymi danymi i pseudonimizacją

- wprowadzenie szczegółowych wytycznych dotyczących przetwarzania danych wrażliwych i pseudonimizacji, w szczególności w sektorze zdrowia i usług publicznych,
- zdefiniowanie ram prawnych i technicznych dla legalnego i bezpiecznego „otwierania" danych osobowych do celów rozwoju AI.

6. Budowa suwerenności danych i technologicznej

- wskazanie zasad przetwarzania danych w Polsce, w tym klasyfikacja danych według poziomu wrażliwości i określenie zasad przetwarzania danych krytycznych wyłącznie w infrastrukturze krajowej,
- promowanie rozwoju i użycia polskich rozwiązań AI, trenowanych na krajowych danych, przez instytucje publiczne.

7. Rozszerzenie działań edukacyjnych i kompetencyjnych

- wzmocnienie edukacji i kształcenia obywateli niezależnie od platform technologicznych BigTech,
- wprowadzenie mechanizmów wsparcia dla edukacji obywatelskiej w zakresie etycznego i świadomego korzystania z AI oraz danych.

Łączę wyrazy szacunku

Mirosław Wróblewski
Prezes Urzędu
Ochrony Danych Osobowych