PREZES
URZĘDU OCHRONY
DANYCH OSOBOWYCH
Mirosław Wróblewski

Warszawa,

DOL.401.354.2024

Pan
Krzysztof Gawkowski
Wiceprezes Rady Ministrów
Minister Cyfryzacji

ePUAP: /MAiC/SkrytkaESP

Szanowny Panie Premierze,

w odpowiedzi na pismo z 16 października 2024 r., znak: DP.MC.WLA.0211.35.2024, działając na podstawie art. 57 ust. 1 lit. c) rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679[1] oraz art. 51 ustawy o ochronie danych osobowych[2], uprzejmie informuję, że do przedstawionego **projektu ustawy o systemach sztucznej inteligencji** (UC71), zwanego dalej projektem ustawy, Prezes Urzędu Ochrony Danych Osobowych jako organ nadzorczy zgłasza następujące uwagi.

Szeroki zakres regulacji aktu w sprawie sztucznej inteligencji[3] (dalej również jako: rozporządzenie 2024/1689) tworzy potrzebę wprowadzenia w krajowym porządku prawnym szeregu rozwiązań zapewniających stosowanie ww. aktu, przy jednoczesnym zapewnieniu spójności systemowej regulowanej materii i obowiązujących przepisów. Niewątpliwie jednym z najistotniejszych zagadnień, które prawodawca unijny przekazał do uregulowania na poziomie krajowym, jest ukształtowanie na szczeblu krajowym skutecznej struktury nadzoru nad poszczególnymi systemami sztucznej inteligencji.

[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.), dalej: „rozporządzenie 2016/679".
[2] Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz. U. z 2019 r. poz. 1781).
[3] 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).

Struktura nadzorcza rynku krajowego w obszarze stosowania aktu w sprawie sztucznej inteligencji powinna służyć interesom publicznym. Dlatego ważne jest uwzględnienie w projektowanym modelu nadzoru rynku celów, ról i uprawnień istniejących organów nadzorczych właściwych dla poszczególnych sektorów oraz horyzontalnych obszarów sprawowanego nadzoru.

Przedstawiona w projekcie ustawy koncepcja sprawowania nadzoru nad systemami sztucznej inteligencji w Polsce wymaga – w ocenie Prezesa Urzędu Ochrony Danych Osobowych – **istotnej modyfikacji i dostosowania do postanowień rozporządzenia 2024/1689.**

Podkreślenia wymaga, że prawa podstawowe, których gwarancje ochrony wynikają z Karty praw podstawowych Unii Europejskiej (KPP UE) oraz Traktatu o funkcjonowaniu Unii Europejskiej (TFUE), podlegają szczególnemu nadzorowi w zakresie zastosowań sztucznej inteligencji. Jednym z tych praw jest prawo do ochrony danych osobowych, a jego przestrzeganie podlega kontroli niezależnego organu[4], co wynika nie tylko z art. 8 KPP UE oraz art. 16 TFUE, ale też wprost z art. 51 rozporządzenia 2016/679 oraz przepisów ustawy o ochronie danych osobowych, którym jest w polskim systemie prawa **wyłącznie** Prezes Urzędu Ochrony Danych Osobowych (dalej jako Prezes UODO). Projekt ustawy, kształtując nadzór nad systemami sztucznej inteligencji w Polsce, powinien uwzględniać szczególną pozycję organu nadzorczego do spraw ochrony danych osobowych, wynikającą zarówno z przepisów rozporządzenia 2024/1689, jak i rozporządzenia 2016/679.

I. Niezależność organu ochrony danych.

Podkreślenia wymaga na wstępie, że kluczowym atrybutem organu nadzorczego ds. ochrony danych osobowych w unijnym systemie ochrony danych jest jego niezależność**,** chroniona gwarancjami prawnymi czerpiącymi źródło w prawie UE (art. 16 TFUE oraz art. 8 KPP UE). Prawna ochrona niezależności organów ochrony danych osobowych ma na celu zapewnienie skuteczności i wiarygodności nadzoru przestrzegania przepisów dotyczących ochrony danych osobowych osób fizycznych i musi być interpretowana w świetle tego celu – na co wielokrotnie zwracał uwagę Trybunał Sprawiedliwości Unii Europejskiej[5]. Niezależność organu ochrony danych osobowych musi być rozpatrywana na kilku płaszczyznach, w tym przede wszystkim w aspekcie niezależności instytucjonalnej, czyli braku jakiejkolwiek podległości wobec

[4] Art. 8 ust. 3 Karty praw podstawowych Unii Europejskiej (Dz. Urz. UE z 2016 r. C 202, s. 391, dalej jako: KPP UE) oraz art. 16 ust. 2 Traktatu o funkcjonowaniu Unii Europejskiej (Dz. Urz. UE z 2016 r. C 202, s.1, dalej jako: TFUE).

[5] Wyrok Trybunału Sprawiedliwości UE z 6.10.2015 r. w sprawie C-362/14, Maximillian Schrems przeciwko Data Protection Commissioner, EU:C:2015:650. Zob. również wcześniejsze wyroki TSUE, chociażby z 9.3.2010 r. w sprawie C-518/07 Komisja przeciwko Niemcom, EU:C:2010:125 czy z 16.10.2012 r. w sprawie C-614/10 Komisja przeciwko Austrii, EU:C:2012:631 oraz z 8.4.2014 r. w sprawie C-288/12 Komisja przeciwko Węgrom, EU:C:2014:237.

innych organów oraz niezależności funkcjonalnej, czyli niepodlegania kontroli innych instytucji w zakresie realizacji swoich kompetencji[6]. Zwraca na to uwagę TSUE w swoim orzecznictwie, w szczególności w ww. wyroku w sprawie C-614/10 Komisja przeciwko Austrii. Trybunał w tym wyroku wskazał, że organy nadzorcze w obszarze ochrony danych osobowych muszą pozostawać poza jakimkolwiek bezpośrednim czy pośrednim wpływem z zewnątrz, mogącym nadawać kierunek ich decyzjom. Z kolei w sprawie C-288/12 Komisja przeciwko Węgrom Trybunał dodał, że nawet potencjalna możliwość wywarcia wpływu na decyzje organu może być wystarczającą przeszkodą w niezależnym wykonywaniu zadań przez organ.

Postanowienia aktu w sprawie sztucznej inteligencji w pełni przyjmują standard niezależności organu nadzorczego określony w rozporządzeniu 2016/679, wskazując w art. 2 ust. 7, że „Prawo Unii w zakresie ochrony danych osobowych, prywatności i poufności komunikacji stosuje się do danych osobowych przetwarzanych w związku z prawami i obowiązkami ustanowionymi w niniejszym rozporządzeniu. Niniejsze rozporządzenie nie ma wpływu na rozporządzenia (UE) 2016/679 lub (UE) 2018/1725, ani na dyrektywy 2002/58/WE lub (UE) 2016/680, bez uszczerbku dla art. 10 ust. 5 i art. 59 niniejszego rozporządzenia”. **Standard ten nie znalazł jednak wyrazu w przepisach projektowanej ustawy, z których nie wynika, że Prezes Urzędu Ochrony Danych Osobowych jest organem wyłącznie właściwym w sprawach ochrony danych osobowych przetwarzanych w ramach systemów sztucznej inteligencji i do niego wyłącznie należy podejmowanie decyzji z zakresu nadzoru nad takimi sprawami**.

Podkreślenia wymaga, że przyznanie wyłącznej kompetencji Komisji Rozwoju i Bezpieczeństwa Sztucznej Inteligencji (dalej jako: Komisja) w zakresie „wykonywania zadań i kompetencji organu nadzoru rynku, określonych w rozporządzeniu 2024/1689”, zgodnie z **art. 11 ust. 1 pkt 7** projektu ustawy, oraz „sprawowania kontroli przestrzegania przepisów rozporządzenia 2024/1689”, zgodnie z **art. 11 ust. 1 pkt 1** projektu ustawy, nie spełnia wymagań odnoszących się do zakresu kompetencji nadzorczych organu ds. ochrony danych osobowych określonych w prawie unijnym, w tym określonych wprost w rozporządzeniu 2024/1689 oraz rozporządzeniu 2016/679**. To przepisy rozporządzenia 2016/679 stanowią podstawę dla nadzoru nad wszystkimi sprawami z zakresu przetwarzania danych osobowych w obszarze regulacji aktu w sprawie sztucznej inteligencji**, zastrzegając wyłączność sprawowania nadzoru w tej materii niezależnemu organowi nadzorczemu, tj. Prezesowi UODO.

Z motywu 10 aktu w sprawie sztucznej inteligencji wynika, że jego celem nie jest wpływanie na stosowanie obowiązującego prawa Unii regulującego przetwarzanie

[6] Dodatkowo należy pamiętać o niezależności personalnej, dotyczącej piastuna organu i jego statusu, ale także niezależności materialnej, czyli gwarancji posiadania właściwych funduszy i zasobów kadrowych i organizacyjnych, umożliwiających sprawne i efektywne wykonywanie zadań. Szczegółowo na ten temat, z odniesieniem do literatury naukowej i orzecznictwa TSUE pisali jeszcze w 2018 r. A. Grzelak i M. Wróblewski, *Niezależność Prezesa Urzędu Ochrony Danych Osobowych w świetle prawa UE*, w: M. Gumularz, K. Kozieł, P. Kozik (red.), Ustawa o ochronie danych osobowych. Przepisy wdrażające Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 (RODO). Komentarz, Warszawa 2018, s. 239-326. Tam też znajdują się liczne odwołania do szerszej literatury i wskazanego orzecznictwa, dotyczących niezależności organu.

danych osobowych, w tym na zadania i uprawnienia niezależnych organów nadzoru właściwych do monitorowania zgodności z tymi instrumentami. Zatem rozporządzenie jasno wskazuje na to, że kompetencje i niezależność organów nadzorczych ds. ochrony danych nie są ograniczane przepisami aktu w sprawie sztucznej inteligencji, a przejrzystego uregulowania tych kwestii należy oczekiwać w przyjmowanych rozwiązaniach krajowych, czego w opiniowanym projekcie zabrakło.

Przebudowy wymaga zatem określona w projekcie ustawy koncepcja nadzoru nad systemami sztucznej inteligencji, która w **art. 7 ust. 2 pkt 3** zakłada **udział przedstawiciela Prezesa Urzędu Ochrony Danych Osobowych w kolegialnym organie nadzoru rynku, jakim ma być Komisja Rozwoju i Bezpieczeństwa Sztucznej Inteligencji**. Choć docenić należy uwzględnienie potrzeby włączenia organu ochrony danych osobowych w proces oceny nadzoru nad systemami sztucznej inteligencji, to jednak, przedstawiciel organu nadzorczego ds. ochrony danych osobowych – ze względu na konieczność zachowania niezależności organu ds. ochrony danych osobowych – **nie może brać udziału w procesie wydawania decyzji przez inny organ inaczej niż w charakterze doradcy czy obserwatora.** Udział przedstawiciela Prezesa UODO w pracach Komisji byłyby zatem możliwy wyłącznie w charakterze eksperta, z możliwością wypowiedzenia się w kwestiach związanych z ochroną danych osobowych, z zastrzeżeniem braku związania go poleceniami /dyspozycjami Przewodniczącego Komisji i przy założeniu nieobjęcia problematyki przetwarzania danych osobowych procesem decyzyjnym Komisji, ze względu na to, iż jest to wyłączna kompetencja Prezesa UODO. Te gwarancje powinny zostać zapisane w ustawie tak, by zapewnić zgodność i spójność zarówno z rozporządzeniem 2024/1689, jak i rozporządzeniem 2016/679.

Ma to istotne znaczenie w związku z **art. 9** projektu ustawy, który przewiduje, że członkowie Komisji wspierają Przewodniczącego Komisji **w wykonywaniu zadań ustawowych, w szczególności w sprawach będących we właściwości podmiotu, którego są przedstawicielami,** a na wniosek Przewodniczącego Komisji, członkowie Komisji przedstawiają działania w zakresie rozwijania, wprowadzania, stosowania, kontrolowania lub nadzorowania systemów sztucznej inteligencji w podmiotu, której są przedstawicielami". Wskazać należy, że **przedstawiciel Prezesa UODO – z racji potrzeby zachowania niezależności, wynikającej wprost z prawa UE – nie może być zobowiązany mocą jakichkolwiek przepisów, w tym projektowanej ustawy, do podejmowania działań na rzecz innego organu ani dostosowywania się do rozstrzygnięć, które potencjalnie mogłyby wkraczać w zakres jego kompetencji.**

Dostrzec przy tym należy, że status Komisji jako nowego organu administracji publicznej ma charakter precedensowy, ponieważ przewiduje, że jej członkami są przedstawiciele innych organów, w tym przedstawiciel Prezesa UODO (**art. 7 ust. 2 pkt 3** projektu ustawy). Przepisy projektowanej ustawy nie regulują przy tym pozycji takiego przedstawiciela, w szczególności w aspekcie swobody podejmowania przez niego decyzji i innych czynności w ramach Komisji, co może być poddane dalszej dyskusji pod kątem zgodności z zasadami prawa administracyjnego i normami konstytucyjnymi

dotyczącymi administracji państwowej, w tym podstawowym warunkiem dotyczącym samodzielności decyzyjnej organu.

W świetle powyższych uwag, **projektowane przepisy wymagają doprecyzowania statusu Prezesa UODO (jego przedstawiciela) w sposób gwarantujący niezależne wykonywanie przez niego zadań wynikających ze wspomnianych wyżej aktów prawa unijnego i krajowego, w tym orzecznictwa TSUE.**

Projektowana ustawa wymaga zatem powtórnej analizy pod kątem spójności oraz jasności nadawanych nią norm kompetencyjnych, jak również kompleksowości proponowanej regulacji, która powinna również czynić zadość konstytucyjnej zasadzie legalności w aspekcie wyznaczania organom władzy publicznej podstaw i granic działania mocą stanowionych przepisów prawa[7].

II. Brak wdrożenia art. 74 ust. 8 rozporządzenia 2024/1689

Projektowana ustawa **nie odzwierciedla także kompetencji Prezesa Urzędu Ochrony Danych Osobowych wynikających wprost z aktu w sprawie sztucznej inteligencji,** co rodzi obawy o zgodność projektu ustawy z przepisami rozporządzenia**.** Zgodnie z wyraźną dyspozycją **art. 74 ust. 8** rozporządzenia 2024/1689 – w odniesieniu do wymienionych w załączniku III pkt 1 systemów AI wysokiego ryzyka w zakresie, w jakim systemy te są wykorzystywane do celów ścigania przestępstw, kontroli granicznej oraz w kontekście wymiaru sprawiedliwości i demokracji, oraz w odniesieniu do systemów AI wysokiego ryzyka wymienionych w załączniku III pkt 6, 7 i 8 przedmiotowego rozporządzenia – **państwa członkowskie jako organy nadzoru rynku do celów przedmiotowego rozporządzenia wyznaczają właściwe organy nadzorcze ds. ochrony danych** na podstawie rozporządzenia (UE) 2016/679 lub dyrektywy (UE) 2016/680 albo inne organy wyznaczone zgodnie z tymi samymi warunkami ustanowionymi w art. 41–44 dyrektywy (UE) 2016/680. Z treści art. 74 ust. 8 rozporządzenia 2024/1689 wynika, że aby organ nadzorczy do spraw ochrony danych osobowych sprawował nadzór w odniesieniu do systemów w przepisie tym określonych **wymagana jest decyzja ustawodawcy krajowego w tym zakresie**. Rozporządzenie co prawda jest aktem obowiązującym bezpośrednio, o czym stanowi art. 288 TFUE, jednak w tym przypadku prawodawca unijny zdecydował, że stosowne działania powinno podjąć się na poziomie krajowym – formalnie wyznaczyć organ, a także ewentualnie uregulować inne kwestie proceduralne, które się z tym mogą wiązać.

Ustawodawca krajowy jest zatem de iure związany ww. regulacją – **nie może wyznaczyć innego organu niż organ wskazany w art. 74 ust. 8 rozporządzenia 2024/1689** w odniesieniu do wskazanych wyżej systemów AI wysokiego ryzyka. Jeżeli

[7] Uchwała Trybunału Konstytucyjnego z dnia 10 maja 1994 r., sygn. akt W 7/94 (Dz.U. z 1994 r. nr 62, poz. 264).

nie chce narazić się na zarzut nieprawidłowego wdrożenia przepisów unijnych, to musi takie działanie podjąć.

Tymczasem w zakresie spraw, o których mowa w art. 74 ust. 8, projektodawca nakłada jedynie obowiązek współpracy Komisji z Prezesem UODO (**art. 6 ust. 3 pkt 3** projektu), **nie określając nawet jasnych i przejrzystych mechanizmów współpracy.**

W kontekście powyższego oraz wcześniejszych uwag zwrócić uwagę należy również na stanowisko Europejskiej Rady Ochrony Danych, wyrażone w wydanym w lipcu 2024 r. **Oświadczeniu EROD 3/2024 w sprawie roli organów ochrony danych w ramach aktu w sprawie sztucznej inteligencji**[8]. Najistotniejsze w tym kontekście jest zalecenie, aby organy ochrony danych zostały wyznaczone jako organy nadzoru rynku w odniesieniu do systemów sztucznej inteligencji wysokiego ryzyka wykorzystywanych do egzekwowania prawa, zarządzania granicami, sprawowania wymiaru sprawiedliwości i procesów demokratycznych, a zatem kwestii, o których mowa w art. 74 ust. 8 rozporządzenia 2024/1689. EROD wskazała dodatkowo, że państwa członkowskie powinny rozważyć wyznaczenie organów ochrony danych jako organów nadzoru rynku również w odniesieniu do innych systemów sztucznej inteligencji wysokiego ryzyka, z uwzględnieniem opinii krajowego organu ochrony danych, w szczególności w przypadku gdy te systemy sztucznej inteligencji wysokiego ryzyka znajdują się w sektorach, które mogą mieć wpływ na prawa i wolności osób fizycznych w odniesieniu do przetwarzania danych osobowych. Organy ochrony danych, o ile zostały wyznaczone jako organy nadzoru rynku, powinny zostać wyznaczone jako pojedyncze punkty kontaktowe dla społeczeństwa i ich odpowiedników na szczeblu państw członkowskich i UE. Podkreślono, że organy ochrony danych powinny odgrywać istotną rolę w egzekwowaniu aktu w sprawie sztucznej inteligencji, ponieważ większość systemów sztucznej inteligencji wiąże się z przetwarzaniem danych osobowych.

III. Ryzyko dualizmu rozstrzygnięć.

Przepisy rozporządzenia 2016/679 dotyczą nadzoru nad sprawami z zakresu przetwarzania danych osobowych regulowanymi przepisami aktu w sprawie sztucznej inteligencji. Ochrona danych osobowych przetwarzanych przez systemy sztucznej inteligencji jest zatem materią, która podlega kompetencjom organu nadzorczego ds. ochrony danych na mocy rozporządzenia 2016/679. Już obecnie organy nadzorcze – w tym Prezes UODO – podejmują działania wobec operatorów systemów sztucznej inteligencji, którzy nie spełniają swoich obowiązków w procesach przetwarzania danych, w tym ochrony danych, jak np. w zakresie realizacji obowiązku informacyjnego wynikającego z art. 13 rozporządzenia 2016/679 w zakresie, w jakim wykorzystywane w uczeniu algorytmów są dane przekazywane przez użytkowników w ramach interakcji z usługami takimi, jak Chat GPT.

[8] https://www.edpb.europa.eu/news/news/2024/edpb-adopts-statement-dpas-role-ai-act-framework-eu-us-data-privacy-framework-faq_pl (dostęp: 19.11.2024).

Dlatego też – niezależnie od ostatecznego kształtu projektowanej ustawy – dochodzenie praw osób, których dane dotyczą, czy zgłaszanie naruszeń będzie rozpatrywane zgodnie z przepisami rozporządzenia 2016/679, a przepisy rozporządzenia 2024/1689 wyraźnie to potwierdzają.

W związku z tym, kolejnym istotnym zagadnieniem, do którego należy się odnieść, są te **przepisy projektowanej ustawy, które dotyczą nakładania się kompetencji wynikających z obu unijnych regulacji**, tj. rozporządzenia 2016/679 oraz z aktu w sprawie sztucznej inteligencji. Żaden z tych aktów nie stanowi lex specialis wobec drugiego.

Zapewniając w porządku krajowym stosowanie aktów prawa unijnego dotyczących sztucznej inteligencji **nie można zatem pomijać uprawnień Prezesa UODO i jego wiodącej roli w zakresie ochrony danych osobowych**. W tym miejscu wskazać należy na wyrok TSUE w sprawie C-252/21 Meta Platforms[9], który dotyczy współpracy organu ochrony konkurencji z organem ds. ochrony danych w Niemczech. Trybunał wskazał na konieczność zapewnienia poszanowania kompetencji organu nadzorczego ds. ochrony danych w szerokim zakresie ochrony danych osobowych wraz z jego wyłączną kompetencją wykładni przepisów rozporządzenia 2016/679. Stanowisko Trybunału powinno być uwzględniane we wszelkich sprawach dotyczących przetwarzania danych osobowych. Organ nadzorczy ds. ochrony danych musi być uwzględniany we wszystkich działaniach innych organów/podmiotów publicznych, które mają związek z ochroną danych. Implikuje to, jak wyżej wskazano, potrzebę doprecyzowania warunków i form współpracy.

1) Postępowanie przed organem nadzoru.

Rozdział 4 projektu ustawy dotyczy postępowania przed organem nadzoru. Zgodnie z **art. 49 ust. 2** Komisja wszczyna postępowanie m.in. na podstawie skargi. W **art. 50 ust. 4** projektu ustawy wskazuje się, że rozpatrując skargę Komisja może współpracować z organami, o których mowa w art. 6 ust. 3 (czyli m.in. z Prezesem UODO). Projektodawca nie zakłada natomiast przekazywania sprawy według właściwości (np. do organu właściwego w sprawie ochrony danych osobowych). Projektowany art. 50 ust. 4 może powodować wątpliwości interpretacyjne, a w konsekwencji potencjalny konflikt kompetencyjny w przedmiocie rozpatrywania spraw związanych z przetwarzaniem danych osobowych, np. gdy naruszenie aktu w sprawie sztucznej inteligencji będzie wymagało również rozpatrzenia naruszenia rozporządzenia 2016/679. Sprawa w zakresie przetwarzania danych osobowych powinna być, zgodnie z art. 65 § 1 ustawy z 14 czerwca 1960 r. Kodeks postępowania administracyjnego (Dz. U. z 2024 r. poz. 572), przekazana do organu właściwego, tj. do organu ds. ochrony danych osobowych. Przy czym należy mieć na uwadze, że z treści art. 50 projektu ustawy wynika, że skardze należałoby przypisać znaczenie zawiadomienia o nieprawidłowościach w celu wszczęcia postępowania z urzędu, a nie skargi w sprawie

[9] Wyrok TSUE z 4 lipca 2023 r. w sprawie C-252/21 Meta Platforms Inc. przeciwko Bundeskartellamt, EU:C:2023:537.

indywidualnej (zgodnie z definicją strony postępowania w **art. 51 ust. 1** projektu ustawy). Zauważyć należy, że w przypadku, gdy systemy sztucznej inteligencji będą przetwarzać dane osobowe, postępowanie takie musi odbywać się zgodnie z zasadami przetwarzania danych osobowych przewidzianymi w rozporządzeniu 2016/679.

Projektodawca w przepisach projektu ustawy o systemach sztucznej inteligencji dotyczących postępowania przed organem nadzoru nie wskazuje jakimi przesłankami powinien kierować się podmiot danych czy administrator kierując sprawę do Komisji i organu nadzorczego ds. ochrony danych. Możliwe jest zatem skierowanie sprawy do dwóch organów równolegle, czego należy spodziewać się tym bardziej, jeśli obowiązujące przepisy nie będą precyzyjnie regulowały tego zagadnienia. Tak skonstruowane przepisy rozdziału 4 będą powodowały szereg ryzyk, m.in. mogą doprowadzić do różnych ocen prawnych (wydawania różnych decyzji administracyjnych) w odniesieniu do tych samych stanów faktycznych.

2) Sąd ochrony konkurencji i konsumentów.

W **art. 57 ust. 1** projektu ustawy wskazuje się, że: „Od decyzji Komisji przysługuje odwołanie do Sądu Okręgowego w Warszawie – sądu ochrony konkurencji i konsumentów". W ocenie organu nadzorczego ds. ochrony danych przekazanie do właściwości sądu ochrony konkurencji i konsumentów jednego rodzaju spraw w zakresie ochrony danych (spraw w obszarze systemów sztucznej inteligencji) może powodować **rozbieżności w kształtowanych** orzeczeniach. Projektowane rozwiązanie może doprowadzić do **dualizmu rozstrzygnięć sądowych**. Rozstrzyganie spraw dotyczących systemów sztucznej inteligencji przez sąd wskazany w art. 57 projektu ustawy oraz spraw z zakresu ochrony danych osobowych przez sąd administracyjny może doprowadzić do **różnych ocen prawnych tych samych stanów faktycznych**, co w konsekwencji może doprowadzić do powstania **niepewności prawnej**.

3) Zgłaszanie incydentów.

Projekt ustawy w **rozdziale 5** dotyczy **obowiązku zgłaszania incydentów związanych z działaniem systemów sztucznej inteligencji**. Obowiązek wskazany w **art. 61** projektu ustawy jest zbieżny z procedurami zgłaszania naruszeń ochrony danych osobowych przewidzianymi w rozporządzeniu 2016/679. Zgodnie z art. 33 ww. rozporządzenia administrator jest zobowiązany zgłaszać naruszenia ochrony danych osobowych do organu nadzorczego w terminie 72 godzin od ich wykrycia, chyba że jest mało prawdopodobne, aby naruszenie to skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych. W ocenie organu nadzorczego ds. ochrony danych incydenty związane z systemami AI, które prowadzą do naruszeń ochrony danych, powinny być zgłaszane zgodnie z procedurami przewidzianymi przez rozporządzenie 2016/679.

Zwrócić uwagę należy, że projektowane **przepisy ustawy nie wskazują jednak konkretnego terminu na zgłoszenie incydentu od momentu wykrycia incydentu**. Określenie terminu usprawniłoby skuteczne zarządzanie incydentami.

Art. 63 projektu ustawy wymaga, aby Przewodniczący Komisji przekazywał

zgłoszenie oraz informacje, o których mowa w art. 61 projektowanej ustawy: 1) koordynatorowi do spraw usług cyfrowych, 2) ministrowi właściwemu do spraw informatyzacji, 3) organowi właściwemu do spraw ochrony danych osobowych, 4) właściwemu CSIRT MON, CSIRT NASK lub CSIRT GOV – z wyłączeniem informacji stanowiących tajemnice prawnie chronione, w tym stanowiących tajemnicę przedsiębiorstwa. **Z przepisów projektowanej regulacji nie wynika jednak, jakie dalsze działania powinien podjąć Prezes Urzędu Ochrony Danych Osobowych, który otrzymywałby takie zgłoszenie. Uzupełnienia wymaga zarówno termin na zgłoszenie incydentu oraz wyjaśnienie czy procedura wskazana w tym przepisie wyklucza zgłoszenie naruszenia danych osobowych w ciągu 72 godzin bezpośrednio do Prezesa UODO.**

Zauważyć ponadto należy, że **terminologia dotycząca incydentów jest używana niekonsekwentnie** – w niektórych przepisach pojawia się ogólne określenie „incydent," a w innych „poważny incydent", co wymaga doprecyzowania (w art. 3 w definicjach mowa jest o poważnym incydencie w rozumieniu art. 3 pkt 49 rozporządzenia 2024/1689).

4) Interpretacje generalne i indywidualne.

Zgodnie z **art. 11 ust. 1 pkt 13** projektu ustawy do zadań Komisji należy **dokonywanie interpretacji generalnych i indywidualnych**. Wydawanie na zlecenie Komisji interpretacji generalnych i indywidualnych przez przedstawiciela Prezesa UODO będącego członkiem Komisji w opinii organu nadzorczego ds. ochrony danych budzi wątpliwości pod kątem stosowania art. 57 rozporządzenia 2016/679, w którym została określona niezależność. Prezes UODO nie może być związany interpretacją wydaną przez Komisję w kwestiach dotyczących ochrony danych osobowych.

5) Wyłączenie stosowania przepisów rozporządzenia 2016/679.

Zgodnie z **art. 26 ust. 7** projektu ustawy, **„**Przetwarzanie przez Komisję i podmioty, o których mowa w art. 7 ust. 2 ustawy, danych, o których mowa w ust. 3, nie wymaga realizacji obowiązków wynikających z art. 15, art. 16, art. 18 ust. 1 lit. a i d oraz art. 19 zdanie drugie rozporządzenia 2016/679, jeżeli uniemożliwiłoby to realizację zadań Komisji". Zwrócić uwagę należy, że **wyłączenia** stosowania przepisów rozporządzenia 2016/679 przewidziane są jedynie w treści art. 13, 14 i 17 rozporządzenia 2016/679. Każde wyłączenie, aby mogło być uznane za mające rację bytu, musi wynikać z obowiązujących przepisów prawa, a jednocześnie – dla równowagi ograniczania pewnych elementów praw podstawowych – muszą być zapewnione odpowiednie instrumenty prawne dla poszanowania praw jednostki. Z kolei ewentualne **ograniczenia** stosowania rozporządzenia 2016/679 mogą następować w dość szerokim, ale nie w pełnym zakresie oraz tylko o ile spełnione zostaną warunki z art. 23, w szczególności dla

zapewnienia poważnych celów, o których stanowi art. 23 ust. 1 rozporządzenia 2016/679. Całkowite wyłączenie praw osób, których dane dotyczą nie jest zatem dopuszczalne ani na gruncie na gruncie rozporządzenia 2016/679, choć jest możliwe ich ograniczenie[10].

Bez wątpienia zatem proponowany przepis projektu ustawy powinien być na nowo przeanalizowany w celu zapewnienia zgodności przepisów krajowych z zasadami wynikającymi z art. 23 rozporządzenia 2016/679 i jego treścią, zwłaszcza, że art. 2 ust. 7 zdanie drugie aktu w sprawie sztucznej inteligencji wprost wskazuje, że „Niniejsze rozporządzenie nie ma wpływu na rozporządzenia (UE) 2016/679 lub (UE) 2018/1725, ani na dyrektywy 2002/58/WE lub (UE) 2016/680, bez uszczerbku dla art. 10 ust. 5 i art. 59 niniejszego rozporządzenia". Skoro akt w sprawie sztucznej inteligencji nie określa w sposób szczegółowy praw osób, których dane dotyczą, zastosowanie będą w tym zakresie mieć przepisy rozporządzenia 2016/679, co jedynie oznacza, że ww. omawiana propozycja musi być przedmiotem ponownej, szczegółowej analizy i korekty jeśli przepisy nowej ustawy mają być jasne i przejrzyste.

III. Pozostałe uwagi.

Wątpliwości budzi **art. 26 ust. 1** projektu ustawy, który stanowi, że „W celu realizacji zadań, o których mowa w art. 11 ust. 1, Komisja przetwarza dane osobowe, obejmujące także dane określone w art. 9 ust. 1 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 […], w zakresie i w celu niezbędnym do realizacji tych zadań". Wskazać należy, że obowiązek administratora w kwestii zabezpieczenia danych osobowych na mocy rozporządzenia 2016/679 dotyczy wszystkich danych osobowych (a nie jedynie danych szczególnych kategorii). Wskazanie w projekcie tego wymogu w odniesieniu wyłącznie do danych szczególnej kategorii jest zbędne i może prowadzić do wątpliwości

[10] Wymagane jest jednak spełnieniu następujących przesłanek: 1) odpowiednio skonstruowane przepisy aktu prawnego – a nie jedynie przepis wskazujący pełne wyłączenie stosowania całych aktów prawnych. Ustawodawca może ograniczać ściśle określony wskazanymi przepisami rozporządzenia 2016/679 zakres praw i obowiązków, tj. tych, które przewidziane są w art. 12-22 i w art. 34 oraz art. 5 rozporządzenia 2016/679; 2) akt prawny ograniczający w ww. zakresie prawa i obowiązki musi zawierać przepisy odpowiadające prawom i obowiązkom przewidzianym w art. 12-22 rozporządzenia 2016/679; 3) wprowadzane w ww. sposób ograniczenie nie może naruszać istoty podstawowych praw i wolności (a za takie uznać należałoby aktualne brzmienie art. 30 projektu ustawy); 4) wprowadzane w ww. sposób ograniczenie musi być w demokratycznym społeczeństwie środkiem niezbędnym i proporcjonalnym, 5) ograniczenie służyć może jednemu z celów przewidzianych w art. 23 ust. 2 lit a) – j) rozporządzenia 2016/679. Dodatkowo, niezbędne jest – dla wprowadzania zgodnego z przepisami rozporządzenia 2016/679 ograniczenia praw – aby akt prawny, o którym mowa w ust. 1, zawierał szczegółowe przepisy przynajmniej - w stosownym przypadku - o: a) celach przetwarzania lub kategorii przetwarzania; b) kategoriach danych osobowych; c) zakresie wprowadzonych ograniczeń; d) zabezpieczeniach zapobiegających nadużyciom lub niezgodnemu z prawem dostępowi lub przekazywaniu; e) określeniu administratora lub kategorii administratorów; f) okresach przechowywania oraz mających zastosowanie zabezpieczeniach z uwzględnieniem charakteru, zakresu i celów przetwarzania lub kategorii przetwarzania; g) ryzykach naruszenia praw lub wolności osoby, której dane dotyczą; oraz h) prawie osób, których dane dotyczą, do uzyskania informacji o ograniczeniach, o ile nie narusza to celu ograniczenia.

interpretacyjnych w zakresie zabezpieczania danych zwykłych. Projektodawca nie powinien różnicować zabezpieczania danych ze względu na ich kategorię.

Projektodawca **nie uzasadnił 5-letniego terminu** określonego w **art. 26 ust. 5** projektu ustawy dotyczącego usuwania lub anonimizowania przez Komisję danych osobowych pozyskanych w związku z nadzorem nad systemami sztucznej inteligencji. Zgodnie z zasadą ograniczenia przechowywania, o której mowa w art. 5 ust. 1 lit. e rozporządzenia 2016/679[11] projektowany przepis wymaga analizy i wyjaśnienia, bowiem dane powinny być przechowywane przez okres nie dłuższy, niż jest to niezbędne do celów, w których dane te są przetwarzane. Nie przesądzono, czy dotyczy to przechowywania danych osobowych w związku z prowadzonymi postępowaniami czy realizacją innych zadań Komisji. Projektodawca nie bierze pod uwagę także stosowania przepisów o archiwizacji, którym podlegać będą dokumenty wytwarzane i opracowywane w ramach działania tego organu publicznego.

Jak wynika z projektowanego **art. 26 ust. 6**, w celu realizacji zadań określonych w rozporządzeniu 2024/1689 i projektowanej ustawie Komisja i pracownicy podmiotów, o których mowa w art. 7 ust. 2, mogą przekazywać sobie wzajemnie dane, o których mowa w ust. 3, w zakresie niezbędnym do realizacji tych zadań i współpracować z organem nadzorczym ds. ochrony danych osobowych. Jednocześnie w rozdziale 3 projektu ustawy zawarte są regulacje, które mają określać zasady przeprowadzania kontroli przez Komisję, mającej na celu ustalenie zgodności działalności podmiotów obowiązanych do przestrzegania przepisów rozporządzenia 2024/1689 i ustawy z tymi przepisami. Przepis w obecnym brzmieniu jest niezrozumiały, wymagający wyjaśnienia z perspektywy zasady rozliczalności nad danymi osobowymi gromadzonymi w różnych systemach. Pracownicy podmiotów nie mogą przekazywać sobie danych, bo to nie oni są administratorami danych.

Wątpliwości budzi proponowane brzmienie **art. 26 ust. 9** w związku z ukształtowanym w projekcie ustawy statusem Biura Komisji i samej Komisji. Analizy i określenia wymaga status tych podmiotów w procesach przetwarzania danych (któremu podmiotowi należy przypisać status administratora oraz w jakim zakresie), co w związku z funkcjonalną definicją administratora wynikać powinno przede wszystkim z precyzyjnie określonych w projektowanych przepisach zadań i kompetencji.

Zwrócić uwagę należy także na **art. 3** projektu ustawy, w której znajduje się słownik definicji legalnych. W ocenie Prezesa UODO jest on zbędny i sprzeczny z zasadami techniki prawodawczej. Ustawa nie nadaje nowego brzmienia tym definicjom, natomiast wprost odsyła do treści aktu w sprawie sztucznej inteligencji, które do przepisy

[11] Zgodnie z art. 5 ust. 1 lit. e rozporządzenia 2016/679 dane muszą być przechowywane w formie umożliwiającej identyfikację osoby, której dane dotyczą, przez okres nie dłuższy, niż jest to niezbędne do celów, w których dane te są przetwarzane; dane osobowe można przechowywać przez okres dłuższy, o ile będą one przetwarzane wyłącznie do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych na mocy art. 89 ust. 1, z zastrzeżeniem że wdrożone zostaną odpowiednie środki techniczne i organizacyjne wymagane na mocy niniejszego rozporządzenia w celu ochrony praw i wolności osób, których dane dotyczą ("ograniczenie przechowywania").

i tak będą stosowane bezpośrednio – powtarzanie ich w treści ustawy może wręcz rodzić wątpliwości pod kątem zakazu powtarzania przepisów rozporządzeń UE w prawie krajowym, jeżeli samo rozporządzenie tego nie przewiduje.

Podobnie **art. 4 pkt 3** projektu ustawy należałoby doprecyzować w zakresie wprowadzonego w nim wyłączenia stosowania ustawy zgodnie z art. 2 pkt 6 aktu w sprawie sztucznej inteligencji, w którym użyto sformułowania „wyłącznie" do celów badań naukowych.

III. Uprawnienia organów ochrony praw podstawowych.

Zgodnie z treścią art. 77 ust. 1 aktu w sprawie sztucznej inteligencji krajowe organy lub podmioty publiczne, **które nadzorują lub egzekwują przestrzeganie obowiązków wynikających z prawa Unii w zakresie ochrony praw podstawowych**, w tym prawa do niedyskryminacji, w odniesieniu do wykorzystywania systemów AI wysokiego ryzyka, o których mowa w załączniku III, **są uprawnione do wystąpienia z wnioskiem o przedstawienie wszelkiej dokumentacji** sporządzonej lub prowadzonej na podstawie przedmiotowego rozporządzenia w przystępnym języku i formacie i uzyskania do niej dostępu, kiedy dostęp do tej dokumentacji jest im niezbędny do skutecznego wypełniania ich mandatów w granicach ich właściwości.

Zgodnie natomiast z art. 77 ust. 2 aktu w sprawie sztucznej inteligencji każde państwo członkowskie wskazuje organy i podmioty publiczne, o których mowa powyżej i podaje ich wykaz do wiadomości publicznej. Jednocześnie państwa członkowskie przekazują ten wykaz Komisji i pozostałym państwom członkowskim oraz na bieżąco go aktualizują.

Tymczasem w dotychczas upublicznionym przez Ministerstwo Cyfryzacji wykazie organów i instytucji publicznych, o których mowa w art. 77 ust. 1 aktu w sprawie sztucznej inteligencji[12] w Polsce nie został wskazany organ nadzorczy ds. ochrony danych, chociaż – jak wynika z informacji przekazanych Prezesowi UODO przez przedstawicieli innych organów nadzorczych – takie działania podejmowane są w innych państwach członkowskich, np. we Francji czy na Malcie.

W świetle powyższych uwag, wzgląd na przepisy prawa, w tym normy prawa unijnego, wymaga uzupełnienia wykazu, o którym mowa w art. 77 ust. 2 aktu w sprawie sztucznej inteligencji i wskazania w nim Prezesa Urzędu Ochrony Danych Osobowych jako organu właściwego z obszaru ochrony praw podstawowych w zakresie realizacji uprawnienia wynikającego z art. 77 ust. 1 ww. aktu. Prezes UODO nie wskazuje przy tym w tym miejscu na konieczne do realizacji tego zadania (i innych wynikających z rozporządzenia 1689/2024 oraz projektu ustawy) zasoby i środki finansowe, których brak mógłby stać na przeszkodzie realizacji nowych kompetencji – powinno to być raczej

[12] Wykaz dostępny jest na stronie internetowej Ministerstwa Cyfryzacji pod linkiem: https://www.gov.pl/web/cyfryzacja/wykaz-organow-i-instytucji-publicznych-w-polsce-z-obszaru-ochrony-praw-podstawowych-w-rozumieniu-rozporzadzenia-20241689-akt-o-sztucznej-inteligencji (dostęp: 13.11.2024)

przedmiotem odrębnych ustaleń, koncentrując się na obowiązkach organów wynikających z przepisów prawa. Należy jednak przypomnieć, że systematyczne pomijanie potrzeb budżetowych organu nadzorczego właściwego ds. ochrony danych osobowych w kontekście realizacji nowych obowiązków (poza projektem ustawy o zarządzaniu danymi) stało się przedmiotem odrębnego wystąpienia do Pana Premiera[13].

Dziękuję uprzejmie Panu Premierowi za przedstawienie niniejszego aktu do zaopiniowania. Liczę na dalszą efektywną dyskusję co do modelu nadzoru nad systemami sztucznej inteligencji i zapewnienia zgodności przyjmowanych rozwiązań z obowiązującymi przepisami prawa unijnego, służąc jednocześnie swoim pełnym wsparciem.

Łączę wyrazy szacunku

Mirosław Wróblewski
Prezes Urzędu
Ochrony Danych Osobowych

/-dokument w postaci elektronicznej
podpisany kwalifikowanym podpisem
elektronicznym/

[13] Pismo Prezesa UODO z 25 września 2024 r.