



**PREZES
URZĘDU OCHRONY
DANYCH OSOBOWYCH**

Mirosław Wróblewski

Warszawa, 20 lipca 2026

DPNT.060.67.2026.WL.KM

**Pani
Katarzyna Bis-Płaza
Sekretarz
Komitet do spraw Cyfryzacji
Ministerstwo Cyfryzacji**

Szanowna Pani Minister,

w związku z pismem z 9 lipca 2026 r., znak: DPIS-WWKS.002.91.1.2026 działając na podstawie art. 57 ust. 1 lit. c) rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679¹ oraz art. 51 ustawy o ochronie danych osobowych² Prezes Urzędu Ochrony Danych Osobowych **do opisu założeń projektu informatycznego** (dalej OZPI) **Referencyjna i bezpieczna infrastruktura wewnątrzadministracyjna oraz Doradczy System Ekspertowy (DSE-L) dla wymiaru sprawiedliwości i struktur adwokatury, wnioskodawca i beneficjent: Kancelaria Prezesa Rady Ministrów, beneficjent: Naczelna Rada Adwokacka** informuje, że:

- **generalnie pozytywnie pod kątem ochrony danych osobowych ocenia przedstawione w OZPI treści,**
- **niemniej jednak przedstawia rekomendacje dotyczące planowanego wykorzystania w projekcie 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 10 maja 2018 r. o ochronie danych osobowych (Dz. U. 2019 r. poz. 1781 ze zm.).

I. Założenia ogólne projektu.

Stosownie do **pkt 1. „Powody podjęcia przedsięwzięcia” ppkt 1.1.**

„Identyfikacja problemu i potrzeb” OZPI planowany projekt informatyczny stanowi duże, horyzontalne przedsięwzięcie wewnątrzadministracyjne nakierowane na głęboką cyfryzację procesów back-office w wymiarze sprawiedliwości oraz strukturach samorządu adwokackiego. Rezygnacja z powszechnej dostępności obywatelskiej na rzecz dedykowanego, lokalnego systemu (on-premise) wynika bezpośrednio z konieczności bezwzględnego spełnienia rygorystycznych, ustawowych wymogów ochrony tajemnicy prawniczej. Wdrożenie systemu DSE-L ma przyczynić się do likwidacji zatorów administracyjnych w sądownictwie poprzez m.in. automatyzację weryfikacji pism na poziomie back-office, ochronę prywatności i danych wrażliwych obywateli, zwiększenie transparentności i dostępności do zasobów wiedzy prawnej, eliminację błędów formalnych na etapie przedprocesowym oraz wyznaczanie standardów etycznych i zgodności z prawem unijnym.

Organ nadzorczy z aprobatą przyjął fakt uwzględnienia przez projektodawcę obszaru dotyczącego ochrony danych osobowych. Przejawem tego jest w szczególności:

- 1) dostrzeżona przez niego potrzeba bezwzględnej ochrony prywatności i danych wrażliwych obywateli: Tradycyjne przetwarzanie danych procesowych niesie ze sobą ryzyko naruszenia tajemnic prawnie chronionych. Izolacja logiczna i zaawansowane algorytmy eliminują ryzyko wycieku danych osobowych poza bezpieczne granice infrastruktury państwowej, w pełni chroniąc konstytucyjne prawa obywateli oraz reżim tajemnicy adwokackiej, obrończej i sędziowskiej (**pkt 1. „Powody podjęcia przedsięwzięcia” ppkt 1.1. „Identyfikacja problemu i potrzeb” oraz 1.2. Opis stanu obecnego OZPI**);
- 2) zaplanowanie przeprowadzenia Testu prywatności systemu oraz przeprowadzenie niezależnych audytów bezpieczeństwa, zgodności i certyfikacji (**3. Kamienie milowe OZPI**),
- 3) uwzględnienie w **pkt 4. Koszty ppkt 4.2. Wykaz poszczególnych pozycji kosztowych – pozycji kosztowej** OZPI: „bezpieczeństwo” oraz „audyt, pilotaż i wdrożenie” uzasadnionych potrzebą zapewnienia m.in. cyberbezpieczeństwa, audytu i bezpieczeństwa,
- 4) zidentyfikowanie w **pkt 5 „Główne ryzyka” pkt. 5.1. „Ryzyka wpływające na realizację przedsięwzięcia”** OZPI istotnych z perspektywy ochrony danych osobowych ryzyk, w tym m.in.:
 - wycieku danych wrażliwych i naruszenia tajemnicy ustawowej,
 - cyberataków typu „prompt injection” na lokalne modele LLM,
 - niezgodności algorytmów AI z nowymi regulacjami prawnymi (w tym AI Act i RODO),
 - niedoszacowania czasu na audyty bezpieczeństwa i wdrożenie pilotażowe.

II. Rekomendacje dotyczące przetwarzania danych osobowych przy wykorzystaniu sztucznej inteligencji (AI)

Projekt Systemu DSE-L w swojej istocie zakłada wykorzystanie narzędzi sztucznej inteligencji. W OZPI podkreśla się m.in., że:

- buduje on przełomową, suwerenną i referencyjną infrastrukturę sztucznej inteligencji dla administracji publicznej (**pkt 1. „Powody podjęcia przedsięwzięcia” ppkt 1.1. „Identyfikacja problemu i potrzeb” oraz 1.2. Opis stanu obecnego OZPI**);
- główną korzyścią z realizacji projektu DSE-L jest głęboka cyfryzacja procesów back-office w wymiarze sprawiedliwości i strukturach adwokatury poprzez wdrożenie referencyjnej infrastruktury bezpiecznego AI na odizolowanym klastrze sprzętowym on-premise; Zwiększenie efektywności procesów administracyjnych w wymiarze sprawiedliwości i samorządzie adwokackim poprzez wdrożenie platformy oraz Doradczego Systemu Ekspertowego opartego na sztucznej inteligencji, wspierającego automatyzację procesów back-office, analizę dokumentów oraz anonimizację orzecznictwa (**pkt. 2. „Efekty przedsięwzięcia” ppkt 2.1. „Cele i korzyści wynikające z realizacji przedsięwzięcia” OZPI**).

Projektodawca jest świadomy tego, że wykorzystywanie AI w planowanym rozwiązaniu informatycznym wymaga podjęcia szeregu działań. Pozytywnie ocenić należy chociażby – wspomniane m.in. w **pkt 5 „Główne ryzyka” pkt. 5.1. „Ryzyka wpływające na realizację przedsięwzięcia” OZPI**– planowane wdrożenie niezależnego audytu etycznego sztucznej inteligencji (AI Fairness) w fazie testowej, które to ma wyprzedzać rynkowe standardy i odpowiada na społeczną potrzebę budowy zaufania do algorytmów podejmujących lub wspomagających decyzje w sektorze publicznym, zgodnie z wymogami unijnego AI Act.

Treść OZPI Systemu DSE-L wskazuje na planowany proces automatyzacji. System ten ma przede wszystkim:

- „zautomatyzować masową anonimizację orzecznictwa za pomocą algorytmów NER” (**pkt. 2 Efekty przedsięwzięcia ppkt 2.1. „Cele i korzyści wynikające z realizacji przedsięwzięcia” OZPI**);
- „automatyzować weryfikację pism procesowych” (m.in. **pkt. 7 „Architektura” ppkt 7.1. „Widok kooperacji aplikacji” OZPI**) – pod względem analizy formalno-prawnej,
- „zapewniać automatyzację asysty decyzyjnej w wymiarze sprawiedliwości przy użyciu zaawansowanego AI (LLM, RAG) (**pkt 2 „Efekty przedsięwzięcia” OZPI**)

W związku z planowaną automatyzacją niektórych procesów związaną z wykorzystywaniem sztucznej inteligencji w przedmiotowym projekcie informatycznym Prezes UODO przypomina i rekomenduje, aby projektodawca zadbał o:

- 1) doprecyzowanie kwestii planowanego wykorzystania wsparcia AI i jego ewentualnego wpływu na przetwarzanie danych osobowych,**

- 2) **jeżeli pewne działania objęte funkcjonowaniem planowanego projektu informatycznego łączą się z możliwością zautomatyzowanego podejmowania decyzji** to należy pamiętać, że w sytuacji pełnej automatyzacji przetwarzania danych osobowych **podmiot danych nie ma wpływu na przebieg takiego procesu**. Dlatego też przepisy art. 22³ rozporządzenia 2016/679 celem ochrony osób, których dane dotyczą, określają uprawnienia ograniczając jego zakres do przypadków „pełnej automatyzacji podejmowania decyzji”, gdy tego rodzaju rozstrzygnięcia wywołują skutki prawne wobec podmiotu danych bądź w podobny sposób istotnie wpływają na niego. Prezes UODO zaleca:
- **zapewnienie interwencji ludzkiej** – osoba kierująca wnioski/pisma powinna mieć prawo do uzyskania wyjaśnień oraz zakwestionowania decyzji wydanej przez algorytm co powinno skutkować ponowną oceną dokonaną przez osobę fizyczną;
 - **transparentność wykorzystywania sztucznej inteligencji** – jeżeli projektodawca przewiduje korzystanie z algorytmów sztucznej inteligencji to osoby kierujące wnioski/pisma muszą być o tym informowane; w takich przypadkach projektodawca powinien zadbać o doprecyzowanie kwestii planowanego wykorzystania wsparcia AI i jego ewentualnego wpływu na przetwarzanie danych osobowych – przy uwzględnieniu zasad przetwarzania danych osobowych, a zwłaszcza zasady zgodności z prawem, rzetelności i przejrzystości⁴ oraz rozliczalności⁵ (art. 5 rozporządzenia 2016/679), a także przeprowadzić wspomniany już wcześniej **test prywatności, w tym uwzględnić ochronę danych w fazie projektowania oraz domyślną ochronę danych (art. 25 rozporządzenia 2016/679)**. Stosownie nowoczesnych technologii (planowane wykorzystanie sztucznej inteligencji) i związane z tym przetwarzanie danych osobowych wymaga przeprowadzania testu prywatności, w tym uwzględnienia ochrony danych zarówno w toku projektowania jak i wykonywania przedmiotowego projektu (art. 35 rozporządzenia 2016/679⁶). **Niezależnie od powyższego niezbędna w takim przypadku będzie również osobna analiza pod względem zgodności**

³ 1. Osoba, której dane dotyczą, ma prawo do tego, by nie podlegać decyzji, która opiera się wyłącznie na zautomatyzowanym przetwarzaniu, w tym profilowaniu, i wywołuje wobec tej osoby skutki prawne lub w podobny sposób istotnie na nią wpływa. 2. Ust. 1 nie ma zastosowania, jeżeli ta decyzja: a) jest niezbędna do zawarcia lub wykonania umowy między osobą, której dane dotyczą, a administratorem; b) jest dozwolona prawem Unii lub prawem państwa członkowskiego, któremu podlega administrator i które przewiduje właściwe środki ochrony praw, wolności i prawnie uzasadnionych interesów osoby, której dane dotyczą; lub c) opiera się na wyraźnej zgodzie osoby, której dane dotyczą. 3. W przypadkach, o których mowa w ust. 2 lit. a) i c), administrator wdraża właściwe środki ochrony praw, wolności i prawnie uzasadnionych interesów osoby, której dane dotyczą, a co najmniej prawa do uzyskania interwencji ludzkiej ze strony administratora, do wyrażenia własnego stanowiska i do zakwestionowania tej decyzji. 4. Decyzje, o których mowa w ust. 2, nie mogą opierać się na szczególnych kategoriach danych osobowych, o których mowa w art. 9 ust. 1, chyba że zastosowanie ma art. 9 ust. 2 lit. a) lub g) i istnieją właściwe środki ochrony praw, wolności i prawnie uzasadnionych interesów osoby, której dane dotyczą.

⁴ Dane osobowe muszą być przetwarzane zgodnie z prawem, rzetelnie i w sposób przejrzysty dla osoby, której dane dotyczą ("zgodność z prawem, rzetelność i przejrzystość").

⁵ Administrator jest odpowiedzialny za przestrzeganie przepisów ust. 1 i musi być w stanie wykazać ich przestrzeganie ("rozliczalność").

⁶ Jeżeli dany rodzaj przetwarzania – w szczególności z użyciem nowych technologii – ze względu na swój charakter, zakres, kontekst i cele z dużym prawdopodobieństwem może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, administrator przed rozpoczęciem przetwarzania dokonuje oceny skutków planowanych operacji przetwarzania dla ochrony danych osobowych. Dla podobnych operacji przetwarzania danych wiążących się z podobnym wysokim ryzykiem można przeprowadzić pojedynczą ocenę.

planowanych operacji przetwarzania z Aktem w sprawie sztucznej inteligencji⁷ (AI Act). Zalecane jest także wzięcie przez projektodawcę pod rozwagę opinii Europejskiej Rady Ochrony Danych (EROD) 28/2024 w sprawie wykorzystania danych osobowych do opracowywania i wdrażania modeli sztucznej inteligencji⁸.

Określono w niej kryteria pozwalające ustalić kiedy i w jaki sposób modele sztucznej inteligencji można uznać za realnie anonimowe oraz jakie metody uniemożliwiające identyfikację osób fizycznych można zastosować, aby zapewnić anonimowość.

Zaznaczyć należy, że odpowiednie środki techniczne i organizacyjne powinny uniemożliwiać stosowanie sztucznej inteligencji w celu niedozwolonego profilowania i zautomatyzowanego podejmowania decyzji (art. 22 ust. 1 rozporządzenia 2016/679).

Ważnym jest, aby użytkownicy korzystający z AI byli we właściwy sposób informowani o sposobie jej funkcjonowania. Pozwoli to administratorowi danych na realizację zasad przetwarzania danych osobowych zwłaszcza zasady: rozliczalności, rzetelności i przejrzystości.

W polskim w polskim porządku prawnym nie została dotychczas uregulowana materia zakresu dopuszczalnego wykorzystywania systemów sztucznej inteligencji opartych na dużych modelach językowych w procesach podejmowania rozstrzygnięć przez podmioty publiczne. Kwestia ta ma szczególne znaczenie w przypadku wykorzystywania takich systemów do wspomagania czynności mogących wpływać na prawa lub obowiązki jednostek – osób fizycznych, zarówno obsługiwanych obywateli, jak i obsługujących, tj. pracowników / urzędników. Wydawanie rozstrzygnięć przy istotnym wsparciu systemów AI – nawet jeżeli ostateczna decyzja pozostaje formalnie w gestii człowieka – może prowadzić do zwiększenia ryzyka naruszenia praw i wolności osób fizycznych, tj. dóbr rozumianych szeroko, nie tylko prawa do autonomii informacyjnej jednostki czy prawa do prywatności. W **pkt. 6 Otoczenie prawne OZPI** nie przewiduje się dla jego realizacji konieczności dokonywania żadnych zmian w prawie powszechnie obowiązującym. **Zdaniem organu nadzorczego niezbędne jest podjęcie prac legislacyjnych, celem stworzenia kompleksowej regulacji dającej podstawy prawne do stosowania zaawansowanych modeli sztucznej inteligencji przez podmioty publiczne, zwłaszcza zważywszy na kontekst przetwarzania danych osobowych przez systemy sztucznej inteligencji w procesach decyzyjnych, także wtedy, gdy nie dochodzi do pełnej automatyzacji procesu.**

Podkreślić należy, że przedstawiane uwagi Prezesa Urzędu Ochrony Danych Osobowych mają charakter eksperckich wskazówek dla projektodawcy, który podejmuje

⁷ 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).

⁸ Określono w niej kryteria pozwalające ustalić kiedy i w jaki sposób modele sztucznej inteligencji można uznać za realnie anonimowe oraz jakie metody uniemożliwiające identyfikację osób fizycznych można zastosować, aby zapewnić anonimowość. Treść opinii znajduje się na stronie internetowej: https://www.edpb.europa.eu/documents/opinion-of-the-board-art-64/opinion-282024-on-certain-data-protection-aspects-related-to_pl [dostęp 2.07.2026 r.].

decyzję co do ostatecznego kształtu projektowanych rozwiązań i odpowiada za zapewnienie ich zgodności z przepisami o ochronie danych osobowych. Wyrażam nadzieję, że uwzględnienie niniejszych uwag będzie pomocne w tym procesie i przyczyni się do podwyższenia poziomu ochrony danych osobowych w przedmiotowym projekcie informatycznym.

Z wyrazami szacunku,

z up. Prezesa Urzędu
Ochrony Danych Osobowych
Zastępczyni Prezesa
Urzędu Ochrony Danych Osobowych
dr hab. Agnieszka Grzelak
/-dokument w postaci elektronicznej
podpisany kwalifikowanym podpisem elektronicznym/