



Warszawa, 02-04-2025

**PREZES**  
**URZĘDU OCHRONY**  
**DANYCH OSOBOWYCH**  
**Mirosław Wróblewski**

sygn. DPNT.060.47.2025.WL.MP

**Pani**  
**Katarzyna Bis-Płaza**  
**Sekretarz**  
**Komitetu Rady Ministrów**  
**do spraw Cyfryzacji**  
**Ministerstwo Cyfryzacji**

ePUAP: /MAiC/SkrytkaESP

Szanowna Pani Sekretarz,

w odpowiedzi na pismo z 31 marca br., znak DPiS.WWKS.002.75.1.2025, działając na podstawie art. 57 ust. 1 lit. c) rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679<sup>1</sup> oraz art. 51 ustawy o ochronie danych osobowych<sup>2</sup>, do przedstawionego **opisu założeń projektu informatycznego „Blżej Teatru – Digitalizacja i udostępnianie zasobów archiwalnych Teatru Polskiego we Wrocławiu”** (dalej jako „OZPI” lub „projekt”) organ nadzorczy – Prezes Urzędu Ochrony Danych zgłasza następujące uwagi.

Projekt zakłada cyfrowe odwzorowanie teatralnych zasobów archiwalnych, w tym w dużej mierze materiałów wizualnych i fonicznych, tj. multimediiów, plakatów, fotografii, kostiumów, zapisów audio-wideo. Zdigitalizowane materiały mają być następnie upowszechniane. Ze względu na specyficzny charakter tego rodzaju materiałów, digitalizacja i ich udostępnianie w wielu przypadkach wiązać będzie się z przetwarzaniem danych osobowych, w tym także potencjalnie danych

---

<sup>1</sup> 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 jako rozporządzenie 2016/679.

<sup>2</sup> Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz. U. z 2019 r. poz. 1781).

szczególnych kategorii (art. 9 ust. 1<sup>3</sup> rozporządzenia 2016/679). Z tego względu warto wziąć pod uwagę kilka istotnych kwestii związanych z ochroną danych osobowych już na wstępnym etapie wdrażania projektu.

Pozytywnie należy ocenić, że OZPI zakłada „**inicjalny**” **test prywatności**<sup>4</sup>. Test ten powinien obejmować ocenę skutków dla ochrony danych osobowych (art. 35 ust. 1<sup>5</sup> rozporządzenia 2016/679), która pozwoli na zdiagnozowanie konkretnych ryzyk dla praw i wolności podmiotów danych wynikających z wdrażanych rozwiązań i umożliwi wypracowanie szczegółowych rozwiązań techniczno-organizacyjnych, minimalizujących zidentyfikowane zagrożenia. Ponadto, test prywatności powinien objąć **analizę i dokładny przegląd** mający na celu ustalić czy w zbiorach przeznaczonych do digitalizacji znajdują się dane osobowe podlegające reżimowi przetwarzania z rozporządzenia 2016/679 (w tym szczególnie regułom postępowania z danymi wrażliwymi), a jeżeli tak, to jakie konkretne rozwiązania należy wdrożyć, aby zapewnić zgodność z zasadami przetwarzania określonymi przez rozporządzenie ogólne oraz realizację praw i obowiązków określonych w art. 12-21 tego aktu. Istotnym jest, aby na jak najwcześniejszym etapie opracowany został **wstępny rejestr czynności przetwarzania danych osobowych**, który wykazywałby konkretne kategorie danych osobowych i zakres ich przetwarzania, a przede wszystkim **podstawy prawne, na których przetwarzanie będzie się opierać w przypadku poszczególnych operacji**, uwzględniając przede wszystkim zasady minimalizacji danych i ograniczenia celu (art. 5 ust. 1 lit. b i c<sup>6</sup>). Taka analiza jest szczególnie istotna, biorąc pod uwagę, że materiały, do których odnosi się projekt mają być w przyszłości **upubliczniane**, co wiąże się ze znacznie zwiększonym ryzykiem naruszenia praw podmiotów danych.

---

<sup>3</sup> Zabrania się przetwarzania danych osobowych ujawniających pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych oraz przetwarzania danych genetycznych, danych biometrycznych w celu jednoznacznego zidentyfikowania osoby fizycznej lub danych dotyczących zdrowia, seksualności lub orientacji seksualnej tej osoby.

<sup>4</sup> To jak ważnym aspektem jest test prywatności towarzyszący wdrażaniu systemów teleinformatycznych Prezes UODO wielokrotnie wskazywał w korespondencji z Komitetem, a potrzeba ta została podzielona przez Panią Sekretarz w piśmie z 31 stycznia 2025 r., znak DPiS.WWKS.501.1.1.2025.

<sup>5</sup> 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.

<sup>6</sup> 1. Dane osobowe muszą być:

(...)

b) zbierane w konkretnych, wyraźnych i prawnie uzasadnionych celach i nieprzetwarzane dalej w sposób niezgodny z tymi celami; dalsze przetwarzanie do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych nie jest uznawane w myśl art. 89 ust. 1 za niezgodne z pierwotnymi celami ("ograniczenie celu");

c) adekwatne, stosowne oraz ograniczone do tego, co niezbędne do celów, w których są przetwarzane ("minimalizacja danych");

Z zadowoleniem przyjąć należy, że część z powyższych problemów została już zidentyfikowana przez projektodawcę w tabeli ryzyk wpływających na realizację projektu (pkt 5.1, wiersz pierwszy). Również pozytywnie należy ocenić, że w założeniach projektu przewidywane jest wdrożenie środków bezpieczeństwa. W tym kontekście warto zwrócić uwagę, że bezpieczeństwo danych nie powinno być rozpatrywane jedynie w kategoriach ich utraty czy awarii, ale również pod względem zachowania ich poufności, prawdziwości, integralności i bezpieczeństwa wedle kryteriów z rozporządzenia 2016/679 (art. 32 ust. 1<sup>7</sup>, art. 5 ust. 1 lit. d i f<sup>8</sup>).

Ze względu na specyficzny charakter materiałów podlegających digitalizacji, wartym rozszerzenia jest aspekt **szczególnych zabezpieczeń przed niedozwolonymi formami przetwarzania**. Digitalizowane będą w znacznej mierze materiały wizualne i audio-wizualne. Rozstrzygnięcia wymaga zatem, czy narzędzia i system prowadzące do cyfrowego odzwierciedlenia cyfrowego określonych materiałów będą działały w oparciu o **środki specjalnego przetwarzania technicznego**, polegającego na analizowaniu cech fizycznych, fizjologicznych, behawioralnych, szczegółów wizerunku lub głosu. Takie narzędzia wiązać się będą bowiem z **przetwarzaniem danych biometrycznych** w rozumieniu rozporządzenia 2016/679, które to stanowią dane szczególnej kategorii i podlegają specjalnemu reżimowi przetwarzania. Celem przeciwdziałania niepożądanemu lub niedozwolonemu przetwarzaniu danych biometrycznych powinny zostać **przewidziane stosowne środki zapobiegawcze, eliminujące takie ryzyko**.

Projekt nie odwołuje się do kwestii związanych z wykorzystywaniem **systemów sztucznej inteligencji (SI)**, chociaż ze względu na powyżej opisane zagrożenia warto, aby kwestia ta została rozstrzygnięta. Jeżeli przewidywane narzędzia mają funkcjonować w oparciu o algorytmy AI, konieczna jest osobna

<sup>7</sup> Uwzględniając stan wiedzy technicznej, koszt wdrażania oraz charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie wystąpienia i wadze, administrator i podmiot przetwarzający wdrażają odpowiednie środki techniczne i organizacyjne, aby zapewnić stopień bezpieczeństwa odpowiadający temu ryzyku, w tym między innymi w stosownym przypadku:

- a) pseudonimizację i szyfrowanie danych osobowych;
- b) zdolność do ciągłego zapewnienia poufności, integralności, dostępności i odporności systemów i usług przetwarzania;
- c) zdolność do szybkiego przywrócenia dostępności danych osobowych i dostępu do nich w razie incydentu fizycznego lub technicznego;
- d) regularne testowanie, mierzenie i ocenianie skuteczności środków technicznych i organizacyjnych mających zapewnić bezpieczeństwo przetwarzania.

<sup>8</sup> Dane osobowe muszą być:

(...)

- d) prawidłowe i w razie potrzeby uaktualniane; należy podjąć wszelkie rozsądne działania, aby dane osobowe, które są nieprawidłowe w świetle celów ich przetwarzania, zostały niezwłocznie usunięte lub sprostowane ("prawidłowość");
- f) przetwarzane w sposób zapewniający odpowiednie bezpieczeństwo danych osobowych, w tym ochronę przed niedozwolonym lub niezgodnym z prawem przetwarzaniem oraz przypadkową utratą, zniszczeniem lub uszkodzeniem, za pomocą odpowiednich środków technicznych lub organizacyjnych ("integralność i poufność").

analiza pod względem zgodności planowanych operacji przetwarzania z Aktem w sprawie sztucznej inteligencji (AIA)<sup>9</sup>. W takim przypadku, równolegle do oceny skutków dla ochrony danych osobowych, konieczne jest przeprowadzenie oceny skutków, o której mowa w art. 27 AIA<sup>10</sup>. Wdrażając model systemów opartych o SI warto odwołać się do opinii Europejskiej Rady Ochrony Danych (EROD) 28/2024 z 17 grudnia 2024 r. w sprawie wykorzystywania danych osobowych do opracowywania i wdrażania modeli sztucznej inteligencji<sup>11</sup>, w której określono 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 (obejmujące nie tylko samą konstrukcję modułu, ale i dobór źródeł, proces szkolenia maszynowego, testy odporności, procedury weryfikacji). Stosowne środki techniczne i organizacyjne powinny uniemożliwiać stosowanie SI w celu niedozwolonego profilowania i zautomatyzowanego podejmowania decyzji (art. 22 ust. 1 rozporządzenia 2016/679<sup>12</sup>) czy też przetwarzania danych biometrycznych. Jeżeli sztuczna inteligencja ma być używana na stronie internetowej czy w aplikacji, które służą do udostępniania materiałów, dla zapewnienia właściwej realizacji przez administratora zasad rozliczalności, rzetelności i przejrzystości ważne jest, aby użytkownicy byli w sposób odpowiedni informowani o sposobie funkcjonowania promptów AI.

---

<sup>9</sup> 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).

<sup>10</sup> Przed wdrożeniem systemu AI wysokiego ryzyka, o którym mowa w art. 6 ust. 2, z wyjątkiem systemów AI wysokiego ryzyka przeznaczonych do stosowania w obszarze wymienionym w załączniku III pkt 2, podmioty stosujące będące podmiotami prawa publicznego lub podmiotami prywatnymi świadczącymi usługi publiczne, oraz podmioty stosujące systemy AI wysokiego ryzyka, o których mowa w załączniku III pkt 5 lit. b) i c), przeprowadzają ocenę skutków w zakresie praw podstawowych, jakie może wywołać wykorzystanie takiego systemu. W tym celu podmioty stosujące przeprowadzają ocenę obejmującą:

- a) opis procesów podmiotu stosującego, w których system AI wysokiego ryzyka będzie wykorzystywany zgodnie z jego przeznaczeniem;
- b) opis okresu, w którym każdy system AI wysokiego ryzyka ma być wykorzystywany i opis częstotliwości tego wykorzystywania;
- c) kategorie osób fizycznych i grup, na które może mieć wpływ wykorzystywanie systemu;
- d) szczególne ryzyko szkody, które może mieć wpływ na kategorie osób fizycznych lub grupy osób zidentyfikowane zgodnie z lit. c) niniejszego ustępu, z uwzględnieniem informacji przekazanych przez dostawcę zgodnie z art. 13;
- e) opis wdrożenia środków nadzoru ze strony człowieka, zgodnie z instrukcją obsługi;
- f) środki, jakie należy podjąć w przypadku urzeczywistnienia się tego ryzyka, w tym ustalenia dotyczące zarządzania wewnętrznego i mechanizmów rozpatrywania skarg.

<sup>11</sup> [https://www.edpb.europa.eu/our-work-tools/our-documents/opinion-board-art-64/opinion-282024-certain-data-protection-aspects\\_pl](https://www.edpb.europa.eu/our-work-tools/our-documents/opinion-board-art-64/opinion-282024-certain-data-protection-aspects_pl)

<sup>12</sup> „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”.

Łączę wyrazy szacunku,

Mirosław Wróblewski  
Prezes Urzędu  
Ochrony Danych Osobowych

/dokument w postaci elektronicznej  
podpisany kwalifikowanym podpisem elektronicznym/

Do wiadomości:

**Wnioskodawca**

**Minister Kultury i Dziedzictwa Narodowego**

**ePUAP**