



**PREZES
URZĘDU OCHRONY
DANYCH OSOBOWYCH**
Miroslaw Wróblewski

Warszawa, 02-04-2025

DPNT.060.44.2025.WL.OJ

**Pani
Katarzyna Bis-Płaza**

**Sekretarz Komitetu Rady Ministrów
do spraw Cyfryzacji
Ministerstwo Cyfryzacji**

ePUAP: /MAiC/SkrytkaESP

Szanowna Pani Sekretarz,

w związku z przekazaniem do wiadomości Prezesa Urzędu Ochrony Danych Osobowych pismem z 27 marca 2025 r. (znak: DPiS.WWKS.002.53.1.2025), dotyczącym opisu założeń projektu informatycznego **„e-Kultura. Cyfrowa transformacja zbiorów specjalnych Biblioteki Uniwersyteckiej w Warszawie oraz Biblioteki Uniwersytetu Muzycznego Fryderyka Chopina”** (dalej: „projekt”), skierowanego do zaopiniowania przez osoby uczestniczące w posiedzeniach Komitetu Rady Ministrów do spraw Cyfryzacji, działając na podstawie art. 57 ust. 1 lit. c) rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679¹ (dalej: „rozporządzenie 2016/679”) oraz art. 51 ustawy o ochronie danych osobowych², organ nadzorczy zgłasza następujące uwagi.

Zgodnie z deklaracjami zawartymi w dokumencie opisu założeń projektu informatycznego (OZPI) projekt jako cel zakłada digitalizację i udostępnienie cennych i unikatowych zasobów kultury a także rozszerzenie funkcjonalności systemu biblioteki cyfrowej Crispa poprzez modyfikację jej poszczególnych modułów systemu. Do metod

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.).

² Ustawa z 10 maja 2018 r. o ochronie danych osobowych (Dz. U. z 2019 r. poz. 1781).

pomiaru KPI wnioskodawca planuje wykorzystać oprogramowanie monitorujące Google Analytics (pkt. 2.1).

Jednocześnie, jak wskazano w OZPI (pkt. 7), „CRISPA Portal (moduł prezentacji obiektów) – zostanie zmodyfikowany w obszarze prezentacji obiektów (wprowadzony zostanie ulepszony interfejs użytkownika, mechanizmy udostępniania treści, logowania i personalizacji oraz nadzór nad uprawnieniami i audytowaniem aktywności użytkowników) oraz pod kątem **zastosowania technologii sztucznej inteligencji (AI)**, szczególnie w zakresie tematowania obiektów cyfrowych oraz poprawy relewancji wyników wyszukiwania; CRISPA REST API (moduł API) zostanie zmodyfikowany dla optymalizacji łączenia się z innymi systemami, w szczególności z systemem Kronik@.”.

Analiza dokumentu OZPI wskazuje, że dokument ten nie zawiera informacji dotyczących sposobu interakcji użytkowników będących osobami fizycznymi z projektowanym systemem informatycznym. W szczególności z dokumentu nie wynika jakie dane osobowe użytkowników mają być pobierane dla interakcji z tym systemem, a także czy będą przetwarzane przy wykorzystaniu poszczególnych rozwiązań w tym systemie generujących ryzyko dla prywatności (np. wykorzystywanie oprogramowania monitorującego Google Analytics, zastosowanie technologii sztucznej inteligencji).

Prezes Urzędu Ochrony Danych Osobowych dostrzega więc konieczność wprowadzenia zmian w dokumencie OZPI w zakresie informacji dotyczących sposobu interakcji użytkowników będących osobami fizycznymi z projektowanym systemem informatycznym. W szczególności organ nadzorczy wnosi o **uzupełnienie OZPI o informację czy (tak/nie) w związku z realizacją projektu będą przetwarzane dane osobowe użytkowników (ew. innych osób), a jeżeli tak, to w jakim celu, w jaki sposób i jakiego rodzaju mają być to dane**. Jeżeli realizacja projektu będzie wiązała się z przetwarzaniem danych osobowych zawarte w OZPI rozwiązania powinny zostać rozbudowane i gwarantować tym danym bezpieczeństwo, a także przewidywać odpowiednie zabezpieczenia praw i wolności osób, których dane dotyczą zgodnie z

zasadami ochrony danych osobowych ukształtowanymi w art. 5 rozporządzenia 2016/679³, a także przy uwzględnieniu art. 22 rozporządzenia 2016/679⁴.

Jednocześnie należy pozytywnie ocenić uwzględnienie przez wnioskodawcę w projekcie, zaplanowanego na styczeń 2026 r., „inicjalnego” testu prywatności, który ma zostać powtórzony w 2028 r., co pozwoli zweryfikować zasadność wykorzystywania w projekcie planowanego zakresu danych, ocenić ryzyka związane z przetwarzaniem tych danych, a także prawidłowość sporządzonej oceny kierunków zmian otoczenia prawnego przez wnioskodawcę. Test ten zawierający ocenę skutków dla ochrony danych powinien

³ Zgodnie z art. 5 ust. 1 rozporządzenia 2016/679 dane osobowe muszą być: a) przetwarzane zgodnie z prawem, rzetelnie i w sposób przejrzysty dla osoby, której dane dotyczą ("zgodność z prawem, rzetelność i przejrzystość"); 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"); 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"); e) 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"); 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"). Zgodnie z art. 5 ust. 2 rozporządzenia 2016/679 Administrator jest odpowiedzialny za przestrzeganie przepisów ust. 1 i musi być w stanie wykazać ich przestrzeganie ("rozliczalność").

⁴ Zgodnie z art. 22 rozporządzenia 2016/679 „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.”.

spełniać wymogi art. 25 ust. 1⁵ i art. 35 (w szczególności ust. 1⁶ oraz ust. 10⁷) rozporządzenia 2016/679.

Biorąc jednak pod uwagę dostrzeżone przez Prezesa Urzędu Ochrony Danych Osobowych braki w dokumencie OZPI zasadnym jest rozważanie przez wnioskodawcę przesunięcie „inicjalnego” testu prywatności na bliższy termin, tj. w roku 2025, ponieważ informacje z tego testu pomogą właściwie uzupełnić ww. dokument w zakresie informacji dotyczących przetwarzania danych osobowych w ramach projektowanych rozwiązań i ewentualnie podjąć działania w celu zmian w otoczeniu prawnym.

Jednocześnie wykorzystanie w ramach projektu technologii sztucznej inteligencji sprawia, że projekt ten powinien zostać także oceniony przez pryzmat zapewnienia

⁵ 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 zagrożenia wynikające z przetwarzania, administrator – zarówno przy określaniu sposobów przetwarzania, jak i w czasie samego przetwarzania – wdraża odpowiednie środki techniczne i organizacyjne, takie jak pseudonimizacja, zaprojektowane w celu skutecznej realizacji zasad ochrony danych, takich jak minimalizacja danych, oraz w celu nadania przetwarzaniu niezbędnych zabezpieczeń, tak by spełnić wymogi niniejszego rozporządzenia oraz chronić prawa osób, których dane dotyczą.

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.

⁷ Ust. 1–7 nie mają zastosowania, jeżeli przetwarzanie na mocy art. 6 ust. 1 lit. c) lub e) ma podstawę prawną w prawie Unii lub w prawie państwa członkowskiego, któremu podlega administrator, i prawo takie reguluje daną operację przetwarzania lub zestaw operacji, a oceny skutków dla ochrony danych dokonano już w ramach oceny skutków regulacji w związku z przyjęciem tej podstawy prawnej – chyba że państwa członkowskie uznają za niezbędne, by przed podjęciem czynności przetwarzania dokonać oceny skutków dla ochrony danych.

stosowania Aktu w sprawie sztucznej inteligencji⁸, z uwzględnieniem art. 27, także ust. 4 tej regulacji⁹, tj. oceny skutków systemów AI wysokiego ryzyka dla praw podstawowych.

W opinii organu nadzorczego wnioskodawca powinien więc rozważyć dokonanie takiej oceny w dokumencie opisu założeń projektu informatycznego, jeżeli uzna, że systemy te będą spełniać przesłanki systemów AI wysokiego ryzyka, o których mowa w art. 6 Aktu w sprawie sztucznej inteligencji.

Należy także zwrócić uwagę, że wykorzystanie w ramach projektu oprogramowania monitorującego Google Analytics, jeżeli to wykorzystanie będzie wiązało się z przetwarzaniem danych osobowych, może rodzić ryzyka zarówno w sferze Cyberbezpieczeństwa, jak i w związku z przekazywaniem danych osobowych do państw trzecich, które powinny być oszacowane w ocenie skutków dla ochrony danych osobowych.

W przypadku podjęcia prac legislacyjnych nad projektami aktów prawa, które stanowiłyby podstawę dla projektowanego rozwiązania Urząd Ochrony Danych Osobowych deklaruje swoje eksperckie wsparcie.

⁸ 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).

⁹ 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.

2. Obowiązek ustanowiony w ust. 1 ma zastosowanie do wykorzystania systemu AI wysokiego ryzyka po raz pierwszy. W podobnych przypadkach podmiot stosujący może polegać na wcześniej przeprowadzonych ocenach skutków dla praw podstawowych lub na istniejących ocenach skutków przeprowadzonych przez dostawcę. Jeżeli w trakcie wykorzystania systemu AI wysokiego ryzyka podmiot stosujący uzna, że którykolwiek z elementów wymienionych w ust. 1 uległ zmianie lub nie jest już aktualny, podmiot ten podejmuje niezbędne kroki w celu aktualizacji informacji.

3. Po przeprowadzeniu oceny, o której mowa w ust. 1 niniejszego artykułu, podmiot stosujący powiadamia organ nadzoru rynku o jej wynikach, przedkładając jako element tego powiadomienia wypełniony wzór, o którym mowa w ust. 5 niniejszego artykułu. W przypadku, o którym mowa w art. 46 ust. 1, podmioty stosujące mogą zostać zwolnione z obowiązku dokonania powiadomienia.

4. Jeżeli którykolwiek z obowiązków ustanowionych w niniejszym artykule został już spełniony w wyniku oceny skutków dla ochrony danych przeprowadzonej zgodnie z art. 35 rozporządzenia (UE) 2016/679 lub art. 27 dyrektywy (UE) 2016/680, ocena skutków w zakresie praw podstawowych, o której mowa w ust. 1 niniejszego artykułu, stanowi uzupełnieniem tej oceny skutków dla ochrony danych.

5. Urząd ds. AI opracowuje wzór kwestionariusza, w tym za pomocą zautomatyzowanego narzędzia, aby ułatwić podmiotom stosującym spełnianie ich obowiązków wynikających z niniejszego artykułu w sposób uproszczony.

Łączę wyrazy szacunku,

Mirosław Wróblewski
Prezes Urzędu Ochrony Danych Osobowych

/ - dokument w postaci elektronicznej podpisany
kwalifikowanym podpisem elektronicznym/