PREZES
URZĘDU OCHRONY
DANYCH OSOBOWYCH

Mirosław Wróblewski

Warszawa,**01 czerwca 2026**

DPNT.060.23.2026.WL.KM

Pani
Katarzyna Bis-Płaza
Sekretarz
Komitet do spraw Cyfryzacji

Szanowna Pani Minister,

w związku z pismem z 26 maja 2026 r., znak: DPIS-WWKS.002.36.1.2026 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] Prezes Urzędu Ochrony Danych Osobowych **do opisu założeń projektu informatycznego (dalej OZPI) „Cyfrowe Dziedzictwo Statystyki: digitalizacja i udostępnienie archiwalnych i naukowych zasobów statystyki publicznej" (dalej „projekt") – wnioskodawca: Kancelaria Prezesa Rady Ministrów, beneficjent: Główny Urząd Statystyczny** zgłasza następujące uwagi.

Projekt w swojej istocie – zgodnie z **pkt. 1 „Powody podjęcia projektu" ppkt 1.1. „Identyfikacja problemu i potrzeb"** OZPI – przewiduje przede wszystkim cyfryzację materiałów archiwalnych, bibliotecznych Głównego Urzędu Statystycznego (GUS) i Centralnej Biblioteki Statystycznej (CBS). Przypuszczalnie dane, które będą poddawane procesowi cyfryzacji w ramach realizacji projektu będą miały jedynie statystyczny wymiar. Niemniej jednak **nie można wykluczyć przetwarzania w ramach projektu także danych osobowych** (np. danych osobowych użytkowników korzystających z zasobów zgromadzonych w planowanym rozwiązaniu informatycznym). Dlatego też autorzy projektu

[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.).

powinni zadbać **o dokonanie realnej i dogłębnej analizy tego czy w związku z realizacją projektu informatycznego nie będzie dochodziło do przetwarzania danych osobowych.** Jeżeli okaże się, że dane osobowe będą przetwarzane to wnioskodawca powinien określić jak będzie wyglądał **„cykl życia" danych osobowych jakie mają być przetwarzane przy wykorzystaniu przedmiotowego projektu (od momentu ich pozyskania do ich usunięcia). Niezbędnym jest aby określone zostały role i obowiązki (**w tym też te z obszaru ochrony danych osobowych) **poszczególnych podmiotów, które będą miały realny dostęp do danych znajdujących się w projektowanym rozwiązaniu** (np. będą mogły wprowadzać/modyfikować /usuwać/ przeglądać znajdujące się w niej informacje, w tym dane osobowe). Przedmiotowy projekt informatyczny powinien zapewniać zachowanie poufności, integralności, kompletności oraz dostępności danych osobowych, które będą w nim przetwarzane.

Stosownie do pkt 4 „Koszty" ppkt. 4.2. „Wykaz poszczególnych pozycji kosztowych" nazwa pozycji kosztowej „Bezpieczeństwo: Testy bezpieczeństwa" OZPI w uzasadnieniu pozycji kosztowej (przeznaczenie) pojawia się informacja o analizie zgodności z obowiązującymi standardami ochrony danych zagwarantuje spełnienie wymagań technicznych. Kwestie bezpieczeństwa, w tym wspominane testy są w kontekście art. 32 rozporządzenia 2016/679 – istotnym elementem planowanego projektu informatycznego. Zauważyć jednocześnie należy, że **raporty z testów bezpieczeństwa oraz dokumentacji potwierdzającej zgodność z wymogami ochrony danych osobowych nie są jedynymi środkami technicznymi i organizacyjnymi, jakie powinny być brane pod rozwagę. Istotne są także inne aspekty wynikające z przepisów rozporządzenia 2016/679**.

Wnioskodawca zidentyfikował ryzyka związane z przetwarzaniem danych w **pkt. 5. „Główne ryzyka" 5.1. Ryzyka wpływające na realizację projektu** OZPI istniej ryzyko niewystarczającego poziomu migracji danych do nowego systemu bibliotecznego. Natomiast w **ppkt. 5.2. projektu Ryzyka wpływające na utrzymanie efektów** utrata danych na skutek awarii lub zniszczenia infrastruktury oraz niezwykle ogólnie zagrożenia związane z bezpieczeństwem danych/cyberbezpieczeństwem (wzrost zagrożeń/wystąpienie nowych rodzajów zagrożeń). Wyodrębnienie ryzyk z tego obszaru należy ocenić pozytywnie. Niemniej jednak organ nadzorczy **rekomenduje aby wnioskodawca wskazał jakie konkretnie ryzyka związane z przetwarzaniem danych osobowych mogą być w przedmiotowej sprawie zidentyfikowane.** Dotyczy to zwłaszcza obszarów takich jak nieuprawniony dostęp, wyciek lub nieuprawniona modyfikacja. Jednocześnie powinien on też określić jakie środki techniczne i organizacyjne będą wdrożone w celu ich skutecznego ograniczenia lub minimalizacji ich potencjalnych skutków.

W świetle treści **pkt 6 „Otoczenie prawne" (tabela)** OZPI wskazano, że planowany projekt informatyczny nie będzie wymagał zmiany żadnych przepisów prawa. Organ nadzorczy uprzejmie przypomina, że przetwarzanie danych osobowych przy wykorzystaniu nowego rozwiązania informatycznego nie może funkcjonować w oderwaniu od ram prawnych. **Przetwarzanie danych osobowych przy wykorzystaniu nowego rozwiązania informatycznego musi znaleźć odzwierciedlenie w przepisach prawa, w**

aspekcie sposobów przetwarzania danych osobowych. Niezbędnym jest przeprowadzenie przez jego projektodawców faktycznego testu prywatności w procesie tworzenia prawa (art. 35 rozporządzenia 2016/679), **w tym realnej oceny skutków dla ochrony danych (art. 25 ust. 1 rozporządzenia 2016/679) dotyczącej sposobów przetwarzania danych osobowych w przewidywanym projekcie informatycznym. Rozważenia wymaga przyjęcie w przepisach rangi ustawowej informacji o wykorzystaniu planowanych rozwiązań informatycznych**. W przepisach tego aktu prawnego powinny być określone – przy uwzględnieniu zasad przetwarzania danych osobowych określonych w art. 5 rozporządzenia 2016/679 (zwłaszcza zasady minimalizacji danych oraz celowości ich przetwarzania), ale i wymogów wynikających z art. 6 ust. 3 rozporządzenia 2016/679 – tym bardziej, że przetwarzanie danych osobowych ma następować przez podmiot publiczny albo dla realizacji celów publicznych (art. 6 ust. 1 lit c i e rozporządzenia 2016/679), w szczególności:

- **w jakim celu/celach będą one przetwarzane;**
- a także **kogo dane osobowe (jakich podmiotów danych), a także w jaki sposób oraz w jakim zakresie będą w nim przetwarzane**.

Nadto niezbędnym jest określenie w przepisach także m.in. tego:

- **na jakich zasadach odbywać się będzie ewentualne przekazywanie (udostępnianie) danych osobowych do instytucji współpracujących**,
- **okresów retencji informacji, w tym danych osobowych** (art. 5 ust. 1 lit e) rozporządzenia 2016/679) przetwarzanych w tych systemach.

Istotne jest rozpoznanie ról poszczególnych podmiotów (interesariuszy, zwłaszcza w kontekście listy przepływów informacji, w tym danych osobowych) **w procesach przetwarzania danych osobowych i przyjęcie takich regulacji prawnych, które będą odzwierciedlać faktyczne przetwarzanie danych osobowych, adekwatnie do przypisanych podmiotom zadań, praw i obowiązków związanych z przetwarzaniem danych osobowych, z uwzględnieniem ww. przepisów rozporządzenia 2016/679.**

Nadto, zgodnie pkt 6 „Otoczenie prawne" (tabela) ppkt 12 OZPI 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) NIE wymaga zmian z uwagi na wdrożenie projektu informatycznego**. W ocenie organu nadzorczego nigdy nie będzie dochodzić do sytuacji, w której planowane przyjęcie przez polską administrację publiczną projektu informatycznego będzie skutkowało koniecznością zmiany tego typu aktu na poziomie europejskim.** Błędnym i niewłaściwym jest choćby kierunkowe przyjmowanie (odpowiedź TAK/NIE), że projektowane rozwiązanie może mieć wpływ na treść czy na zmianę regulacji rozporządzenia 2016/697. Dlatego też w części opisu projektu informatycznego odnoszącym się do otoczenia prawnego nie jest rekomendowanym zamieszczanie informacji o jego wpływie na rozporządzenie 2016/697. Ten punkt wymaga usunięcia Ta część opisu służy w swojej istocie bardziej wskazaniu aktów na których treść wprowadzenie (i wdrożenie) projektu informatycznego będzie realnie oddziaływało.

Zgodnie z **pkt. 7 „Architektura" –** tabela odnosząca się do **Listy systemów wykorzystywanych w projekcie** OPZI wnioskodawca określił, że zmiany związane z realizacją projektu informatycznego łączą się z jednej strony z tworzeniem nowego systemu (System Biblioteczny CBS, System Archiwum GUS), modyfikacją już istniejących (np. Portal Naukowy GUS), jak i wycofaniem przestarzałych (System Aleph). Działania ta będą łączyły się w szczególności z migracją danych (w tym osobowych), które zostały już pozyskane/wprowadzone. Nadto, stosownie do **pkt 7.2. Kluczowe komponenty architektury rozwiązania w tabeli Lista systemów wykorzystywanych w projekcie w pkt. 1 System Biblioteczny CBS – w kolumnie opis systemu** znajduje się zdawkowa informacja **o „wsparciu AI".** Niestety nie wiadomo na czym to wsparcie ma polegać, jaki model sztucznej inteligencji i w jakim dokładnie celu ma być wykorzystywana. Nie jest również do końca jasnym, czy wsparcie AI ma służyć użytkownikom projektu informatycznego, a w konsekwencji czy planowana do wykorzystania sztuczna inteligencja będzie w jakimkolwiek stopniu przetwarzała dane osobowe. **W opinii organu nadzorczego wnioskodawca powinien zadbać o doprecyzowanie kwestii planowanego wykorzystania wsparcia AI i jej ewentualnego wpływu na przetwarzanie danych osobowych.** W tym celu powinien on – przy uwzględnieniu zasad przetwarzania danych osobowych, a zwłaszcza zasady zgodności z prawem, przejrzystości oraz rozliczalności (art. 5 rozporządzenia 2016/679) – w toku planowanego testu prywatności (**pkt. 3 tabela Kamienie milowe czwarty wers**) pamiętać o konieczności **uwzględnienia ochrony danych w fazie projektowania oraz domyślnej ochroną danych (*privacy by design* oraz *privacy by default*, art. 25 rozporządzenia 2016/679). Stosownie nowoczesnych technologii (planowane wsparcie AI) 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 2016/679).**

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