PREZES
URZĘDU OCHRONY
DANYCH OSOBOWYCH

Mirosław Wróblewski

Warszawa, **09 listopada 2026**

DPNT.060.115.2026

Pani
Katarzyna Bis-Płaza
Sekretarz
Komitetu do spraw Cyfryzacji
Ministerstwo Cyfryzacji

Szanowna Pani Sekretarz,

w związku z przekazanym do wiadomości pismem z 3 listopada 2026 r., znak: DPIS-WWKS.002.203.1.2026, 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], uprzejmie informuję, że do przedstawionego opisu założeń przedsięwzięcia informatycznego **„Bezpieczna komunikacja mobilna dla podmiotów KSC (BKM)”** – wnioskodawca: Minister Cyfryzacji, beneficjent: Ministerstwo Cyfryzacji, Prezes Urzędu Ochrony Danych Osobowych jako organ nadzorczy zgłasza następujące **uwagi**.

[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.).

Jak wynika z przedstawionego opisu założeń, celem przedsięwzięcia jest „optymalizacja procesu podłączania wraz z opracowaniem usługi umożliwiającej automatyzację wnioskowania o dostęp do systemu" SKR-Z [System Komunikacji Rządowej – Zastrzeżone], udostępniającego usługi bezpiecznej komunikacji takie jak mail, komunikator w części jawnej i niejawnej. E-usługą udostępnioną w ramach przedsięwzięcia ma być „wnioskowanie o dołączenie do systemu SKR-Z".

Nie kwestionując zasadności projektowanego rozwiązania i potrzeby usprawnienia procedur podłączania podmiotów do systemu SKR-Z należy wskazać, że:

— w przypadku, gdy z korzystaniem z projektowanego narzędzia wiązało będzie się przetwarzanie danych osobowych (np. wnioskodawców czy użytkowników systemu), to przy jego tworzeniu konieczne jest uwzględnienie poniższych aspektów dotyczących przetwarzania danych osobowych.

1. **Podczas opracowywania nowych projektów czy przedsięwzięć informatycznych, w pierwszej kolejności należy:**

— uwzględnić konstytucyjne standardy: praworządności, źródeł prawa dla regulowania praw i obowiązków, w tym wiążące organy publiczne oraz ochrony prywatności i autonomii informacyjnej jednostki, ew. innych praw podstawowych (art. 7, 31, 47, 51, 87 Konstytucji RP);

Należy podkreślić, że wszelkie ograniczenia tych praw oraz zasady zbierania danych i gospodarowania nimi mogą być określane wyłącznie w drodze aktu rangi ustawy, z poszanowaniem wymogu proporcjonalności, standardów konstytucyjnych

(art. 51 w zw. z art. 31 ust. 3 Konstytucji RP) oraz z art. 6 ust. 3 i motywem 41 rozporządzenia 2016/679[3].

Zważywszy na porządek konstytucyjny i przepisy ogólnego rozporządzenia o ochronie danych uzasadnionym jest, by podstawa prawna zawierała przepisy szczegółowe dostosowujące stosowanie przepisów tego rozporządzenia, w tym: ogólne warunki zgodności z prawem przetwarzania przez administratora; rodzaj danych podlegających przetwarzaniu; osoby, których dane dotyczą; podmioty, którym można ujawnić dane osobowe; cele, w których można je ujawnić; ograniczenia celu; okresy przechowywania; oraz operacje i procedury przetwarzania, w tym środki zapewniające zgodność z prawem i rzetelność przetwarzania.

Na szczególną uwagę zasługuje zwłaszcza **materia przetwarzania szczególnych kategorii danych osobowych** (art. 9 rozporządzenia 2016/679, a w uzasadnionych przypadkach także art. 10 rozporządzenia 2016/679), o ile zakładane projekty / przedsięwzięcia miałyby obejmować przetwarzanie danych osobowych dotyczących wyroków skazujących i czynów zabronionych.

2. **Jeżeli projektowane przedsięwzięcie będzie wiązało się z przetwarzaniem, danych osobowych** konieczne jest również, aby zgodnie z wymogami rozporządzenia 2016/679 w obowiązujących już przepisach lub (w przypadku ich braku) w regulacjach prawnych służących wykonywaniu projektów / uwzględniono:

- jednoznaczne określenie w przepisach rangi ustawowy podstaw prawnych takiego przetwarzania,
- cel / cele, zakres, kategorie przetwarzanych danych,
- krąg podmiotów uprawnionych do ich przetwarzania,

[3] Zgodnie z powołanym przepisem podstawa przetwarzania danych realizowanego w celu wypełnienia obowiązku prawnego lub wykonania zadania w interesie publicznym musi być określona w prawie unijnym lub prawie krajowym. Z kolei zgodnie z motywem 41 „w przypadku gdy w niniejszym rozporządzeniu jest mowa o podstawie prawnej lub akcie prawnym, niekoniecznie wymaga to przyjęcia aktu prawnego przez parlament, z zastrzeżeniem wymogów wynikających z porządku konstytucyjnego danego państwa członkowskiego. Taka podstawa prawna lub taki akt prawny powinny być jasne i precyzyjne, a ich zastosowanie przewidywalne dla osób im podlegających - jak wymaga tego orzecznictwo Trybunału Sprawiedliwości Unii Europejskiej (zwanego dalej "Trybunałem Sprawiedliwości") i Europejskiego Trybunału Praw Człowieka”.

- „cykl życia danych” oraz sposoby ich przetwarzania, od pozyskania po usunięcie, okres przechowywania, retencję,
- odpowiednie, szczególne, związane z rodzajem przetwarzanych danych i adekwatne do ryzyk przetwarzania środki ochrony praw i wolności osób, których dane dotyczą, z uwzględnieniem podwyższonego ryzyka dla prywatności, a także – z uwagi na charakter informacji przetwarzanych w systemie SKR-Z – dla cyberbezpieczeństwa i bezpieczeństwa narodowego.

3. **Jeżeli z realizacją przedmiotowego przedsięwzięcia związane będzie wykorzystywanie danych osobowych przetwarzanych w innych systemach** (zob. pkt 7 opisu założeń) to należy wziąć również pod uwagę, **czy rozwiązania te przewidują łączenie zbiorów danych, co z punktu widzenia przepisów rozporządzenia 2016/679 jest niedozwolone[4]. Konieczne jest zatem określenie wyraźne na poziomie obowiązujących przepisów prawa zasad udostępnienia (przekazywania) danych pomiędzy podmiotami publicznymi.**

Ponadto, dla **funkcjonowania rejestru publicznego i nierozerwalnie z nim związanego przetwarzania gromadzonych w nim danych osobowych wymagane jest:**

- **umocowanie w przepisach rangi ustawowej**,
- **precyzyjne określenie w przepisach celu/celów jego funkcjonowania, a tym samym celu/celów przetwarzania danych osobowych** (brak regulacji w tym zakresie uchybia art. 6 ust. 3 rozporządzenia 2016/679 wskazującemu niezbędne elementy podstawy prawnej przetwarzania danych oraz zasadzie celowości przetwarzania danych osobowych (art. 5 ust. 1 lit. b rozporządzenia 2016/679),
- **określenie w przepisach prawa wyczerpującego katalogu informacji, w danych osobowych, jakie mają znajdować się w tym rejestrze** (powinien on zawierać tylko niezbędny, minimalny zakres danych osobowych (art. 5 ust. 1 lit. c rozporządzenia 2016/679 niezbędny do realizacji celu/celów działania tego rejestru),
- sprecyzowanie, **w jakiej postaci i przy wykorzystaniu jakich narzędzi będzie zasób prowadzony**,

[4] Zgodnie z motywem 31 rozporządzenia 2016/679 żądanie ujawnienia danych osobowych, z którym występują organy publiczne, powinno zawsze mieć formę pisemną, być uzasadnione, mieć charakter wyjątkowy, nie powinno dotyczyć całego zbioru danych ani prowadzić do połączenia zbiorów danych.

- **ustalenie czy zasób będzie pozostawał w relacji z innymi rejestrami publicznymi, a jeśli tak to na jakich zasadach będą między nimi realizowane przepływy danych** (wszelkie niejednoznaczne określenia powinny być wyeliminowane a tryby przekazywania, weryfikacji i udostępniania powinny być kształtowane z poszanowaniem zasady rozliczalności),
- **określenie okresów retencji zawartych w nich informacji, w tym danych osobowych** – przepisy, które określają jawność danych muszą precyzować konkretny okres retencji (przechowywania), aby dane nie widniały w przestrzeni publicznej bezterminowo (art. 5 ust. 1 lit. e rozporządzenia 2016/679),
- **uwzględnienie przepisów ustawy o informatyzacji działalności podmiotów realizujących zadania publiczne[5], jak i dobrych praktyk dotyczących tworzenia rejestrów publicznych** opracowanych przez Ministerstwo Cyfryzacji[6].

Podmioty publiczne, realizujące zadania publiczne z użyciem danych osobowych, nie mogą wykonywać na nich operacji w sposób dowolny – za niewystarczające uznaje się określenie jedynie w prezentowanych założeniach projektów, że: „projekt będzie używał, zmieniał zawartość innych systemów sektora publicznego", zwłaszcza w kontekście **powstawania i funkcjonowania nowych rejestrów, dla realizacji działania których „używane, zmieniane" mają być dane**. **Konieczne jest przy tym wykazanie czy stworzenie kolejnego rejestru jest rzeczywiście niezbędne i czy zamiast tego nie byłoby właściwszym dokonanie zmian w rejestrach już funkcjonujących tak aby nie dochodziło do dublowania baz danych osobowych.**

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 i przyczyni się do podwyższenia poziomu ochrony danych osobowych w przedmiotowym projekcie informatycznym.

---

[5] Dz. U. z 2025 r. poz. 1703.

[6] Zob. Zespół Architektury Informacyjnej Państwa Departamentu Projektów i Strategii Ministerstwa Cyfryzacji, *Rejestry publiczne – dobre praktyki architektoniczne i legislacyjne*, strona internetowa: https://www.gov.pl/web/ia/rejestry-publiczne-dobre-praktyki-architektoniczne-i-legislacyjne [dostęp 26.06.2026 r.].

Łączę wyrazy szacunku

Mirosław Wróblewski

Prezes Urzędu

Ochrony Danych Osobowych

/-dokument w postaci elektronicznej
podpisany kwalifikowanym podpisem elektronicznym/

Do wiadomości:

Pan

Paweł Olszewski

Sekretarz Stanu

Ministerstwo Cyfryzacji