PREZES
URZĘDU OCHRONY
DANYCH OSOBOWYCH

Mirosław Wróblewski

Warszawa, 27-04-2026

DPNT.401.169.2026.WL.PM

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

Szanowna Pani Sekretarz,

w związku z pismem z 22 kwietnia 2026 r. znak: DPiS.WWKS.002.48.1.2026, przekazującym do wiadomości Prezesa Urzędu Ochrony Danych Osobowych informację o skierowaniu do zaopiniowania przez osoby uczestniczące w pracach Komitetu do spraw Cyfryzacji projektu **uchwały Komitetu do spraw Cyfryzacji w sprawie określenia wzoru opisu założeń przedsięwzięcia informatycznego o publicznym zastosowaniu**, 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 UODO jako organ nadzorczy zgłasza uprzejmie następujące uwagi.

W ocenie organu nadzorczego załącznik do projektu uchwały określający uniwersalny **wzór opisu założeń przedsięwzięcia informatycznego o publicznym zastosowaniu** powinien zostać **rozszerzony o elementy regulacji dotyczące wpływu projektu informatycznego na aspekty z zakresu przetwarzania, w tym ochrony danych osobowych**. Są to zagadnienia niezwykle istotne dla zapewnienia zgodności z prawem i powodzenia zasadniczej większości założeń przedsięwzięć informatycznych w sektorze publicznym – dlatego też stworzenie wzoru dla opisu tego rodzaju założeń z uwzględnieniem tego aspektu oraz poniżej przedstawionych elementów jest ważne nie

[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 dnia 10 maja 2018 r. o ochronie danych osobowych (Dz. U. z 2019 r. poz. 1781 ze zm.).

tylko dla prac Komitetu do spraw Cyfryzacji, ale przede wszystkim dla każdego z beneficjentów / wnioskodawców, bardzo często realizujących później rolę projektodawcy – podmiotu odpowiedzialnego za przyjęcie odpowiedniego otoczenia prawnego dla realizacji projektu informatycznego, podstaw prawnych dla projektowanego przetwarzania danych, które nie mieści się w dotychczasowych regulacjach prawnych.

Mowa tu o **regulacjach nieprzewidujących dotąd**, tj. nieobejmujących projektowanych, nowych aspektów, w tym celów i sposobów przetwarzania danych osobowych:

- **podstawy prawnej przetwarzania**, która dla realizacji projektu informatycznego musi być określona w prawie Unii lub w prawie krajowym, któremu podlega administrator (zwłaszcza gdy przetwarzanie danych osobowych jest niezbędne dla wypełnienia obowiązku prawnego czy dla wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi),

- **celu przetwarzania**, który dla realizacji projektu informatycznego musi być określony w tej podstawie prawnej,

- **innych elementów tej podstawy prawnej**, przepisach szczegółowych regulujących **ogólne warunki zgodności z prawem** przetwarzania przez administratora dla realizacji projektu informatycznego,

- **rodzaju** danych podlegających przetwarzaniu dla realizacji projektu informatycznego,

- **osób**, których dane dotyczą dla realizacji projektu informatycznego,

- **podmiotów, którym można ujawnić** dane osobowe, cele, w których można je ujawnić, ograniczenia celu – dla realizacji projektu informatycznego,

- **okresów przechowywania** dla realizacji projektu informatycznego,

- **operacji i procedur przetwarzania**, w tym **środków zapewniających zgodność z prawem i rzetelność przetwarzania**, w tym w szczególnych sytuacjach związanych z przetwarzaniem dla realizacji projektu informatycznego (art. 6).

Aspekty te mają niezwykle istotne znaczenie dla – związanych w wielu przypadkach z realizacją projektu informatycznego – przetwarzania danych **szczególnych kategorii**, które może odbywać się po zapewnieniu podwyższonego reżimu i warunków przetwarzania (art. 9 i art. 10) czy prowadzonego w sposób szczególnie godzących w prawa i wolności, w tym prywatność podmiotów danych (**z użyciem nowoczesnych technologii, w tym w sposób zautomatyzowany, czy poprzez profilowanie** – art. 22 rozporządzenia 2016/679).

Organ nadzorczy wielokrotnie przy opiniowaniu projektów informatycznych kierowanych na posiedzenia Komitetu do spraw Cyfryzacji (uprzednio KRMC) wskazywał, że poszczególni wnioskodawcy powinni przeprowadzać **ocenę skutków dla ochrony**

danych, o której mowa w art. 35 ust. 1 rozporządzenia 2016/679[3], tak aby projekt informatyczny będący przedmiotem prac KdsC uwzględniał ochronę danych w fazie projektowania (art. 25 ust. 1 rozporządzenia 2016/679[4]).

Wielokrotnie również – ze względu na **konieczność wprowadzenia zmian w przepisach powszechnie obowiązującego prawa w związku z pracami nad danym projektem informatycznym** – Prezes UODO wskazywał na konieczność przeprowadzenia testu prywatności i oceny skutków dla ochrony danych już w toku **przyjmowania podstawy prawnej przetwarzania**, która powinna odpowiadać wymogom art. 25 ust. 1 i art. 35 (w szczególności ust. 1 i ust. 10)[5].

Dlatego wzór opisu założeń przedsięwzięcia informatycznego o publicznym zastosowaniu powinien mieć **oddzielny punkt, zawierający informację czy wnioskodawca przeprowadził ocenę skutków dla ochrony danych i po tym, jak jej wynik wpływa na konstrukcję i funkcjonalności projektu informatycznego, w szczególności w obszarze mitygacji ryzyk związanych z przetwarzaniem danych osobowych**.

Konieczne jest również wskazanie czy wnioskodawca (bardzo często realizujący później rolę projektodawcy) zakłada przeprowadzenie oceny skutków dla ochrony danych przy przyjmowaniu odpowiedniej podstawy prawnej przetwarzania.

Informacje o tym powinny być powiązane z **pkt 6** „**Otoczenie prawne**” wzoru opisu założeń przedsięwzięcia informatycznego o publicznym zastosowaniu.

Planowane wykorzystanie dla realizacji projektu informatycznego **technologii sztucznej inteligencji** sprawia, że projekt powinien zostać także oceniony nie tylko pod względem **podstawy prawnej to przewidującej**, ale także przez pryzmat zapewnienia

[3] 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.

[4] 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.

[5] 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 inteligencji[6], z uwzględnieniem jego art. 27 ust. 4, tj. **oceny skutków systemów AI wysokiego ryzyka dla praw podstawowych**[7].

Informacja w tym zakresie również powinna zostać ujęta we wzorze opisu założeń przedsięwzięcia informatycznego o publicznym zastosowaniu.

Organ nadzorczy zwraca również uwagę, że w **pkt 6 „Otoczenie Prawne”**, wnioskodawca wielokrotnie wskazuje na rozporządzenie 2016/679 jako element otocznia prawnego projektu informatycznego, jednocześnie oceniając, że nie wymaga ono zmiany. W ocenie organu nadzorczego nigdy nie będzie dochodzić do sytuacji, w której planowane przyjęcie przez polską administrację publiczną projektu informatycznego będzie skutkowało koniecznością zamiany tego typu aktu na poziomie europejskim.

Dlatego pkt 6 Otoczenie Prawne wzoru opisu założeń przedsięwzięcia informatycznego o publicznym zastosowaniu powinien odnosić się wyłącznie do aktów prawa krajowego, zaś informacje o konieczności zmian zasad przetwarzania danych osobowych w poszczególnych krajowych aktach prawnych, powinny zostać powiązane z kwestią **oceny skutków dla ochrony danych**, która ma być przeprowadzona przy przyjmowaniu podstawy prawnej przetwarzania.

Łączę wyrazy szacunku,

---

[6] 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).

[7] 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.

Mirosław Wróblewski

Prezes Urzędu Ochrony Danych Osobowych

/ - dokument w postaci elektronicznej podpisany kwalifikowanym podpisem elektronicznym/