PREZES
URZĘDU OCHRONY
DANYCH OSOBOWYCH
Mirosław Wróblewski

Warszawa, 31-03-2025

DPNT.060.40.2025

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

ePUAP**:** /MAiC/SkrytkaESP

Szanowna Pani Sekretarz,

w odpowiedzi na pismo przekazane do wiadomości organu nadzorczego do spraw ochrony danych z 26 marca 2025 r. (DPiS.WWKS.002.67.1.2024) dotyczące opisu założeń projektu informatycznego pn.: **Rozbudowa systemu zarządzania infrastrukturą teleinformatyczną statystyki publicznej i cyberbezpieczeństwa (CyberStat)**, skierowane 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) 2016/679[1] (dalej: „rozporządzenie 2016/679") oraz art. 51 ustawy o ochronie danych osobowych[2], Prezes Urzędu Ochrony Danych Osobowych zgłasza następujące uwagi.

Zgodnie z informacjami zawartymi w przekazanym dokumencie planowane jest usprawnienie wybranych procesów back-office, tj. związanych z zarządzaniem IT i bezpieczeństwem informacji. Zmiany te mają się przyczynić do usprawnienia funkcjonowania zdecydowanej większości systemów jednostek służb statystyki publicznej (jssp) niemodyfikowanych w projekcie, w tym rejestrów publicznych REGON i TERYT – stanowiących infrastrukturę krytyczną państwa, np. poprzez podniesienie poziomu ich bezpieczeństwa. Objęte projektem usprawnienia wynikają m.in. z obowiązku

[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, poz. 1781).

spełnienia wymagań wprowadzonych nowymi regulacjami prawnymi na poziomie UE (w tym NIS 2) oraz krajowym (m.in. przygotowywanej nowelizacji ustawy o Krajowym Systemie Cyberbezpieczeństwa), a także dążenia do stałego podnoszenia jakości świadczonych usług publicznych, w tym zapewnienia interoperacyjności i optymalizacji. Realizacja projektu ma usprawnić przekazywanie informacji do Systemu Inwentaryzacji Systemów Teleinformatycznych (SIST) oraz wzmocnić komplementarność systemów GUS z Architekturą Korporacyjną Państwa (AIP).

Z punktu widzenia ochrony danych osobowych najistotniejsza jest jednak informacja, że planowany projekt informatyczny ma związek z przetwarzaniem ogromnej ilości danych, w tym również danych osobowych, przez Prezesa GUS. Zatem działania dążące do poprawy jakości wdrażanych rozwiązań technicznych i organizacyjnych zarządzania bezpieczeństwem informacji podnoszących bezpieczeństwo systemów i realizowanych proces należy ocenić pozytywnie.

Ze względu na wskazane w projekcie przetwarzanie danych osobowych na szeroką skalę, za niezbędne należy uznać przeprowadzenie **testu prywatności** (obejmującego m.in. ocenę skutków dla ochrony danych), odpowiadającego wymogom art. 25 ust. 1 [3] i art. 35 (w szczególności ust. 1 [4] oraz ust. 10 [5]) rozporządzenia 2016/679. We wskazanych w piśmie pkt 2.4 – „Produkty końcowe projektu" i pkt 3 – „Kamienie milowe" mowa jest jedynie m. in. o pozytywnych raportach z testów bezpieczeństwa i wydajności oraz o uzyskanych pozytywnych wynikach testów bezpieczeństwa i wydajności. Należy zauważyć, że zgodnie z przepisami rozporządzenia 2016/679 ocena skutków dla ochrony danych powinna być przeprowadzana nie tylko przed rozpoczęciem przetwarzania, ale i wtedy, gdy zmienia się ryzyko wynikające z operacji przetwarzania[6]. Zasadne jest zatem – również w nawiązaniu do ustaleń zawartych w piśmie Pani Sekretarz z 31 stycznia br.[7] – włączenie testu prywatności (obejmującego m.in. ocenę skutków dla ochrony danych), jako kluczowego dla oceny przetwarzania danych

---

[3] 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.

[4] 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.

[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.

[6] Zgodnie z art. 35 ust. 11 rozporządzenia 2016/679: W razie potrzeby, przynajmniej gdy zmienia się ryzyko wynikające z operacji przetwarzania, administrator dokonuje przeglądu, by stwierdzić, czy przetwarzanie odbywa się zgodnie z oceną skutków dla ochrony danych.

[7] Znak DPiS.WWKS.501.1.1.2025.

osobowych, do opisu założeń, w następujących punktach: pkt 2.4 - Produkty końcowe projektu; pkt 3 – Kamienie milowe; pkt 4.2 - Wykaz poszczególnych pozycji kosztowych; pkt 6 – Otoczenie prawne (w zakresie aktów prawnych umożliwiających przetwarzanie danych). Odpowiednio przeprowadzona analiza powinna pomóc zdiagnozować ryzyka dla praw i wolności podmiotów danych wynikające z przyjmowanych rozwiązań i pozwolić na wypracowanie konkretnych środków zaradczych oraz techniczno-organizacyjnych minimalizując w ten sposób zidentyfikowane zagrożenie. Nie można również pominąć aspektu otoczenia prawnego. Odpowiednio przeprowadzona analiza obowiązujących aktów prawa w przedmiotowym zakresie pozwoli na określenie podstawy prawnej dla każdego z realizowanych procesów związanych z przetwarzaniem danych osobowych. Przez wzgląd na normę zawartą w art. 6 ust. 3 lit b[8] rozporządzenia 2016/679 – dla każdego procesu przetwarzania danych osobowych musi istnieć odpowiednia podstawa prawna, określona w prawie państwa członkowskiego.

Z przekazanego opisu założeń projektu informatycznego nie wynika, aby wdrażane rozwiązania miałyby być wspierane przez systemy sztucznej inteligencji. Podkreślenia jednak wymaga, że jeżeli takie działania miałyby mieć miejsce, niezbędne jest wskazanie na konieczność przeprowadzenia oceny skutków systemów AI wysokiego

[8] Podstawa przetwarzania, o którym mowa w ust. 1 lit. c) i e), musi być określona: a) w prawie Unii; lub b) w prawie państwa członkowskiego, któremu podlega administrator. Cel przetwarzania musi być określony w tej podstawie prawnej lub, w przypadku przetwarzania, o którym mowa w ust. 1 lit. e) - musi być ono niezbędne do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi. Podstawa prawna może zawierać przepisy szczegółowe dostosowujące stosowanie przepisów niniejszego 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, w tym w innych szczególnych sytuacjach związanych z przetwarzaniem, o których mowa w rozdziale IX. Prawo Unii lub prawo państwa członkowskiego muszą służyć realizacji celu leżącego w interesie publicznym, oraz być proporcjonalne do wyznaczonego, prawnie uzasadnionego celu.

ryzyka dla praw podstawowych – zgodnie z art. 27 Aktu w sprawie sztucznej inteligencji[9], jak również art. 22 rozporządzenia 2016/679 dla pełnego poszanowania tej regulacji, która to nie może stracić na znaczeniu.

Łączę wyrazy szacunku,

Mirosław Wróblewski
Prezes Urzędu
Ochrony Danych Osobowych

/ - dokument w postaci elektronicznej podpisany
kwalifikowanym podpisem elektronicznym/

Do wiadomości:

Pan
Grzegorz Karpiński

[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.

Sekretarz Stanu
Zastępca Szefa Kancelarii Prezesa Rady Ministrów

ePUAP