PREZES
URZĘDU OCHRONY
DANYCH OSOBOWYCH
Mirosław Wróblewski

Warszawa, 25-03-2025

DPNT.060.34.2025.WL.MKS

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

ePUAP

Szanowna Pani Sekretarz,

w związku z przekazanym do wiadomości organu nadzorczego pismem z 20 marca br. (znak: DPiS.WWKS.002.60.1.2024) dotyczącym opisu założeń projektu informatycznego **„e-Sanepid**" (wnioskodawca: Minister Zdrowia, beneficjent: Główny Inspektorat Sanitarny; dalej: „opis założeń"), 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.

Z opisu założeń projektu informatycznego e-Sanepid wynika przetwarzanie danych osobowych użytkowników rozbudowywanego Systemu Ewidencji Państwowej Inspekcji Sanitarnej – **SEPIS**, poprzez uwierzytelnienie użytkownika za pomocą Węzła Krajowego, korzystanie przez pracowników Inspekcji z aplikacji klienckiej SEPIS, korzystanie przez obywateli, przedsiębiorców i instytucji z Platformy e-Sanepid, udostępnianie rejestrów publicznych. Oprócz rozbudowy systemu SEPIS w projekcie zaplanowano integrację z innymi systemami, w tym EZD RP, rejestrem PESEL, RDK.

W opisie założeń nie przewidziano konieczności dokonania zmian w prawie (pkt 6 Raportu). Mając zaś na uwadze **charakter przetwarzanych w tym systemie danych, które mogą dotyczyć danych dotyczących zdrowia, a zatem danych szczególnych kategorii**, należy wskazać, że **konieczne jest podjęcie działań**

[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).

legislacyjnych mających na celu określenie właściwej podstawy prawnej dla przetwarzania danych osobowych użytkowników systemu SEPIS. Aktualne regulacje w tym zakresie zostały określone w § 2 rozporządzenia Ministra Zdrowia w sprawie systemów wymiany informacji w zakresie dotyczącym zadań Państwowej Inspekcji Sanitarnej[3], który odnosi się do faktu działania SEPIS w ramach systemu wymiany informacji w zakresie dotyczącym zadań Państwowej Inspekcji Sanitarnej. Dalsze regulacje wynikające z § 3 rozporządzenia wskazują zaś jedynie na techniczne i organizacyjne aspekty utrzymania systemu.

Przetwarzanie danych osobowych przez podmioty publiczne odbywać się bowiem powinno w granicach i na podstawie przepisów prawa, które w sposób precyzyjny wskazują jakie dane będą przetwarzane, w jakim celu, przez jaki okres czasu oraz kto będzie za to przetwarzanie odpowiadał. W przypadku wskazanym w art. 6 ust. 1 lit. c rozporządzenia 2016/679[4], gdy mamy do czynienia z przetwarzaniem danych niezbędnym do wypełnienia obowiązku prawnego ciążącego na administratorze, zastosowanie znajduje art. 6 ust. 3 rozporządzenia 2016/679[5], zgodnie z którym podstawa przetwarzania musi być określona w prawie państwa członkowskiego, któremu podlega administrator.

Z punktu widzenia standardów konstytucyjnych dotyczących prawa do ochrony danych osobowych wynikającego z art. 51 Konstytucji RP, warto podnieść, że sprawy istotne, które muszą zostać uregulowane w przepisach rangi ustawy, obejmują w szczególności warunki dopuszczalności przetwarzania danych osobowych[6].

Ponadto, z uwagi na potencjalne przetwarzanie danych osobowych na **dużą skalę** w projektowanym systemie, w ocenie organu nadzorczego, wskazane jest także przeprowadzenie **testu prywatności, w tym oceny skutków dla ochrony**

---

[3] Rozporządzenie Ministra Zdrowia z 17 października 2014 r. w sprawie systemów wymiany informacji w zakresie dotyczącym zadań Państwowej Inspekcji Sanitarnej (Dz.U. z 2021 r. poz. 226); zgodnie z § 2 pkt 2a rozporządzenia, wykaz systemów wymiany informacji obejmuje następujące systemy: System Ewidencji Państwowej Inspekcji Sanitarnej (SEPIS);

[4] Przetwarzanie jest zgodne z prawem wyłącznie w przypadkach, gdy - i w takim zakresie, w jakim - spełniony jest co najmniej jeden z poniższych warunków: c) przetwarzanie jest niezbędne do wypełnienia obowiązku prawnego ciążącego na administratorze.

[5] 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.

[6] Zob. wyroki z 19 maja 1998 r., sygn. akt U 5/97, 30 lipca 2014 r., sygn. akt K 23/11 oraz 19 lutego 2002 r., sygn. akt U 3/01.

danych (art. 25 ust. 1 [7] oraz 35 ust. 1 [8] rozporządzenia 2016/679), które służą ocenie ryzyka naruszenia praw lub wolności podmiotów danych. Przeprowadzenie testu pozwala na szczegółowe rozeznanie ryzyk towarzyszących przetwarzaniu dla praw i wolności podmiotów danych oraz na wprowadzenie gwarancji te ryzyka eliminujące.

Należy zwrócić uwagę, że opis założeń odnosi się, co prawda, do ww. testu prywatności w zakresie niektórych punktów opisu założeń (produkty końcowe projektu; kamienie milowe; wykaz poszczególnych pozycji kosztowych)[9], jednakże nie oznacza to zwolnienia projektodawcy z **przeprowadzenia analizy obowiązujących przepisów prawa w tym zakresie, które mają wpływ na ochronę danych osobowych** (otoczenie prawne). Istotne jest wykonanie takiego testu prywatności w odniesieniu do tworzonych aktów prawnych również z uwagi na to, że projekt zakłada także udostępnianie danych z różnych, bliżej nieokreślonych, rejestrów publicznych. Przegląd ten pozwoliłby na określenie podstawy prawnej przetwarzania (pozyskiwania, gromadzenia, udostępniania). Takie rozwiązanie przyczyni się jednocześnie do tworzenia projektów informatycznych w zgodzie z przepisami rozporządzenia 2016/679.

Wskazać również trzeba, że z projektu nie wynika jednoznacznie, czy dla realizacji projektu mają być wykorzystywane rozwiązania wykorzystujące do przetwarzania danych osobowych sztuczną inteligencję lub uczenie maszynowe w związku z automatyzacją czynności, analiz i procesów decyzyjnych podejmowanych przez Państwową Inspekcję Sanitarną, niemniej organ nadzorczy zwraca także uwagę na ten aspekt planowanego projektu. Aspekt ten należy **oceniać przez pryzmat zapewnienia stosowania Aktu w sprawie sztucznej inteligencji, ale również przez art. 22 rozporządzenia 2016/679**, która to regulacja nie może stracić na znaczeniu o ile narzędzia sztucznej inteligencji miałyby być wykorzystywane w Państwowe Inspekcji Sanitarnej.

Jeżeli w projektowanym systemie mają być wykorzystywane systemy sztucznej inteligencji wnioskodawca powinien wziąć pod uwagę w szczególności nie tylko przepisy rozporządzenia 2016/679, ale także Akt w sprawie sztucznej inteligencji, którego zapewnienie stosowania w krajowym porządku prawnym jest i będzie niezwykle istotne. Należy bowiem podkreślić, że z art. 27 Aktu w sprawie

---

[7] „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 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”.

[8] „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”.

[9] Zob. pismo Prezesa UODO z 14 stycznia br., znak DOL.071.42.2024

sztucznej inteligencji wynika odrębny obowiązek dokonania oceny skutków systemów AI wysokiego ryzyka dla praw podstawowych. Jeżeli więc realizacja projektu będzie wiązała się z wykorzystaniem systemów AI to, w ocenie organu nadzorczego, wnioskodawca powinien również uwzględnić dokonanie takiej oceny w dokumencie opisu założeń projektu informatycznego. Takie systemy dotyczące przetwarzania danych do wykorzystywania przez Państwową Inspekcję Sanitarną lub w jej imieniu mogą bowiem spełniać przesłanki systemów AI wysokiego ryzyka, o których mowa w art. 6 aktu w sprawie sztucznej inteligencji.

Jednocześnie organ nadzorczy deklaruje swoje eksperckie wsparcie w zakresie zapewnienia zgodności regulacji prawnych z rozporządzeniem 2016/679 w przypadku przedstawienia mu do zaopiniowania projektu ustawy wdrażającej projektowany system informatyczny, a także w dalszych pracach nad projektowanym systemem.

Łączę wyrazy szacunku,

Mirosław Wróblewski
Prezes Urzędu
Ochrony Danych Osobowych

/-dokument w postaci elektronicznej
podpisany kwalifikowanym podpisem
elektronicznym/

Do wiadomości:

Pan
Marek Kos
Podsekretarz Stanu
Ministerstwo Zdrowia
ePUAP