PREZES
URZĘDU OCHRONY
DANYCH OSOBOWYCH
Mirosław Wróblewski

Warszawa, 27 listopada 2024 r.

DOL.060.46.2024.WL.MK

Pani
Wioletta Zwara
Sekretarz Komitetu Rady Ministrów
do spraw Cyfryzacji
Ministerstwo Cyfryzacji

ePUAP

Szanowna Pani Sekretarz,

w związku z przekazanym do wiadomości Prezesa Urzędu Ochrony Danych Osobowych pismem z 18 listopada br. (znak: DPiS.WWKS.002.153.1.2024) dotyczącym projektu informatycznego **"Rozwój centrum kompetencji w zakresie cyfrowego udostępniania i zabezpieczania zbiorów Archiwów Państwowych w Narodowym Archiwum Cyfrowym** - etap I: archiwa centralne i warszawskie**"** (dalej: „projekt informatyczny"), 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 zgłasza uprzejmie następujące poniższe uwagi.

Jak wskazano w opisie założeń projektu, w wyniku podjęcia prac nad projektem, ma nastąpić „modernizacja systemów Szukaj w Archiwach (dalej: SwA), wewnętrznego systemu Zintegrowany System Informacji Archiwalnej (dalej: ZoSIA), a także budowa infrastruktury do digitalizacji oraz przechowywania, zabezpieczania i udostępniania danych".

Mając powyższe na uwadze, należy zwrócić szczególną uwagę, że w przypadku projektowania **rozwiązań z udziałem nowych technologii**, **związanego z przetwarzaniem danych osobowych na szeroką skalę**, projektodawca wykonać

[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 jako „rozporządzenie 2016/679

[2] Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz. U. z 2019 r. poz. 1781).

powinien tzw. test prywatności, w tym **ocenę skutków dla ochrony danych osobowych** (art. 35 ust. 1 i ust. 10 rozporządzenia 2016/679), z uwzględnieniem ochrony danych w fazie projektowania oraz domyślanej ochrony danych (art. 25 ust. 1 i 2 oraz art. 36 rozporządzenia 2016/679). Przeprowadzenie testu pozwoliłoby na szczegółowe rozeznanie ryzyk towarzyszących przetwarzaniu dla praw i wolności podmiotów danych oraz na wprowadzenie gwarancji te ryzyka eliminujące. Nie odnotowano natomiast w udostępnionych dokumentach informacji na temat przeprowadzenia oceny skutków w aspekcie przetwarzania danych osobowych odniesieniu do projektowanych rozwiązań.

W ocenie Prezesa UODO, obecne środowisko technologiczne, ze względu na dynamicznie zmieniające się zagrożenia, **wymaga szczególnej uwagi w odniesieniu do kwestii zapewnienia bezpieczeństwa systemów i aplikacji**, co oznacza podjęcia właściwych działań gwarantujących zabezpieczenie danych osobowych. Tymczasem, należy zauważyć, że w przedstawionym dokumencie w odniesieniu do występujących ryzyk dla realizacji projektu, które wiążą się z gwarancjami bezpieczeństwa modernizowanych systemów, takich jak: nieautoryzowane działanie związane z przetwarzaniem informacji, nieautoryzowany dostęp na poziomie systemów operacyjnych, usług sieciowych i aplikacji (tabela 5.1) postęp technologiczny wpływający na zmiany w sprzęcie oprogramowania, awaria serwerów i systemów oprogramowania (tabela 5.2) - określono jako **„średnie" prawdopodobieństwo ich wystąpienia**, a w przypadku ryzyka utraty danych na skutek awarii lub zniszczenia infrastruktury (tabela 5.2) prawdopodobieństwo wystąpienia określono jako „**znikome**".

W dokumencie nie przewidziano konieczności dokonania zmian w prawie (pkt 6 założeń) oraz przyjmowane jest, że w projekcie będą wykorzystywane inne systemy, np. „Węzeł Krajowy", umożliwiający uwierzytelnianie użytkownika systemu teleinformatycznego, korzystającego z usługi online. Zważywszy zatem na przetwarzanie danych osobowych użytkowników projektowanych / modernizowanych systemów, **niezbędne jest przeprowadzenie analizy obowiązujących przepisów prawa w tym zakresie.** Przegląd ten pozwoli na określenie podstawy prawnej przetwarzania tych danych (pozyskiwania, gromadzenia, udostępniania). Podkreślić należy, że przetwarzanie danych osobowych przez podmioty publiczne odbywać powinno się na podstawie i w granicach przepisów prawa, które w sposób precyzyjny wskażą 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[3], gdy mamy do czynienia z przetwarzaniem danych niezbędnym do wypełnienia obowiązku prawnego ciążącego na administratorze,

[3] 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.

należy mieć na względzie art. 6 ust. 3 rozporządzenia 2016/679[4]. Zgodnie z jego treścią podstawa przetwarzania musi być określona w prawie państwa członkowskiego, któremu podlega administrator.

Z punktu widzenia przepisów rozporządzenia 2016/679 kluczowa jest zatem ocena zaprojektowanych rozwiązań pod względem zapewnienia właściwej podstawy prawnej dla funkcjonowania systemu teleinformatycznego, gwarantującej bezpieczeństwo (w tym cyberbezpieczeństwo), integralność i poufność informacji przetwarzanych w systemie (art. 5 ust. 1 lit f rozporządzenia 2016/679), za których przestrzeganie – zgodnie z zasadą rozliczalności – będzie ponosił odpowiedzialność administrator (art. 5 ust. 2 rozporządzenia 2016/679).

W związku z powyższym, uprzejmie proszę o wzięcie pod uwagę przedstawionych uwag w celu zapewnienia właściwych gwarancji ochrony danych osobowych przetwarzanych w związku z projektowanym / modernizowanym system.

Łączę wyrazy szacunku,

Mirosław Wróblewski
Prezes Urzędu
Ochrony Danych Osobowych

/-dokument w postaci elektronicznej
podpisany kwalifikowanym podpisem
elektronicznym/

Do wiadomości:

Pan
Sławomir Rogowski
Podsekretarz Stanu

[4] 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.

Ministerstwo Kultury i Dziedzictwa Narodowego
ePUAP