GENERALNY INSPEKTOR OCHRONY DANYCH OSOBOWYCH

dr Edyta Bielak-Jomaa

Warszawa, dnia 24 stycznia 2017 r.

DOLiS-041-4/17

Pani
Justyna Duszyńska
Sekretarz
Komitet Rady Ministrów
ds. Cyfryzacji
Ministerstwo Cyfryzacji
ul. Królewska 27
00-060 Warszawa

w odpowiedzi na pismo z dnia 16 stycznia 2017 r. (znak: BZPP-III.002.4.2017) – data wpływu do Biura GIODO 17 stycznia 2017 r. – Generalny Inspektor Ochrony Danych Osobowych (zwany dalej również GIODO lub Generalnym Inspektorem) do opisu założeń projektu informatycznego Platforma Integracji Usług i Danych, zwanego dalej *opisem założeń PIUiD* – z punktu widzenia przepisów ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. 2016 r. poz. 922), zwanej dalej *u.o.d.o.* **– zgłasza następujące uwagi**.

1. **Uwaga do procedury realizacji projektu informatycznego Platforma Integracji Usług i Danych.**

W pkt 6.2 opisu założeń PIUiD *Harmonogram projektu / kamienie milowe* przedstawiony został etap prac nad realizacją projektu informatycznego Platforma Integracji Usług i Danych, zwanego dalej *PIUiD lub projektem*, w którym przewiduje się, że prace legislacyjne na rzecz projektu prowadzone będą od lutego 2017 r. do lutego 2019 r. W trakcie prac legislacyjnych,

niemalże równolegle, nastąpi wybór wykonawcy prac informatycznych (okres od sierpnia 2017 r. do marca 2018 r.), przygotowana zostanie umowa POPC – MC (okres od czerwca 2017 r. do września 2017 r.) oraz wykonywane będą różne prace programistyczne mające na celu zaprojektowanie i uruchomienie projektu.

Generalny Inspektor Ochrony Danych Osobowych, mając świadomość ogromu ilości danych osobowych jakie będą przetwarzane w PIUiD, pragnie zwrócić uwagę wnioskodawcy, że z punktu widzenia nie tylko ochrony danych osobowych ale i zasad wyrażonych w Konstytucji Rzeczypospolitej Polskiej z dnia 2 kwietnia 1997 r. (Dz. U. 1997 r. nr 78 poz. 483 z późn. zm.), zwanej dalej *Konstytucją RP* należy w pierwszej kolejności stworzyć odpowiednią regulację prawną na podstawie, której PIUiD będzie działał a dopiero potem przejść do kolejnych etapów realizacji projektu jakimi są wybór wykonawcy prac informatycznych oraz czynności techniczne związane z jego projektowaniem i uruchamianiem.

Powyższe znajduje swoje potwierdzenie w zasadach prawa ustanowionych w Konstytucji RP. Art. 7 Konstytucji wskazuje, że organy władzy publicznej działają na podstawie i w granicach prawa. Jeżeli, zatem, źródłami powszechnie obowiązującego prawa w Rzeczypospolitej Polskiej zgodnie z art. 87 Konstytucji RP jest są: Konstytucja RP, ustawy, ratyfikowane umowy międzynarodowe oraz rozporządzenia i akty prawa miejscowego a na podstawie art. 51 ust. 1 Konstytucji RP nikt nie może być obowiązany inaczej niż na podstawie ustawy do ujawniania informacji dotyczących jego osoby, to nie możliwe jest zbudowanie takiego systemu bez wcześniejszego stworzenia jego ram prawnych. W opinii GIODO rozwiązanie takie należy uznać za sprzeczne również z przepisami art. 31 ust. 3 Konstytucji RP – zasada wyłączności ustawowej w odniesieniu do przepisów ograniczających możliwość korzystania z konstytucyjnych wolności i praw. Przedmiotowa uwaga podyktowana jest koniecznością respektowania przez wnioskodawcę zasad ochrony zaufania do państwa i stanowionego przez nie prawa oraz zasady bezpieczeństwa prawnego i pewności prawa wywodzonych przez Trybunał Konstytucyjny z art. 2 Konstytucji RP tj. Rzeczpospolita jest demokratycznym państwem prawnym, urzeczywistniającym zasady sprawiedliwości społecznej. Ochrona zaufania do państwa i stanowionego przez nie prawa jest jedną z podstawowych zasad określających stosunki między obywatelem a państwem i zarazem jedną z najważniejszych cech demokratycznego państwa prawnego nierozerwalnie związaną z zasadą bezpieczeństwa prawnego i pewności prawa, która oznacza nie tyle stabilność prawa, co możliwość przewidywania działań organów państwa i związanych z nimi zachowań obywateli.

Zatem, nieprawidłowy w ocenie GIODO, jest obecnie zastosowany proces wprowadzania w życie projektu będący pewnego rodzaju dostosowywaniem otoczenia prawnego do powstającego systemu informatycznego. Tylko jasny, poprawny i precyzyjny przepis prawa może zagwarantować jego komunikatywność względem adresatów. Tak stanowione normy nie powinny

budzić wątpliwości co do treści nakładanych obowiązków i przyznawanych praw co będzie skutkować ich prawidłowym egzekwowaniem.

Generalny Inspektor pragnie przypomnieć wnioskodawcy, że przy tworzeniu przepisów dedykowanych realizacji projektu zastosowanie powinny znaleźć zasady przetwarzania danych osobowych zawarte w art. 26 ust. 1 pkt 1 – 4 u.o.d.o. Są nimi zasada legalności – zapewnienie by przetwarzanie danych osobowych było zgodne z prawem (ust. 1), celowości – zbierane dla oznaczonych, zgodnych z prawem celów i niepoddawane dalszemu przetwarzaniu niezgodnemu z tymi celami (ust. 2); merytorycznej poprawności (ust. 3); adekwatności – adekwatne do celów, w jakich są przetwarzane (ust. 3); ograniczenia czasowego (retencji danych) – przechowywane w postaci umożliwiającej identyfikację osób, których dotyczą, nie dłużej niż jest to niezbędne do osiągnięcia celu przetwarzania (ust. 4). Stąd regulacje prawne muszą precyzyjnie określać zakres danych osobowych, podmioty przetwarzające te dane, cele, dla których będą one przetwarzane oraz zasady ich przetwarzania, w tym retencji. Każde przetwarzanie danych osobowych powinno być również planowane z uwzględnieniem koncepcji ochrony prywatności w fazie projektowania (privacy by design). Idea privacy by design zrodziła się jako sposób spojrzenia na budowanie systemów teleinformatycznych. Polega ona na tym, by od samego początku tworzenia jakiegoś systemu, na każdym etapie, rozważać wpływ tworzonych rozwiązań na sferę prywatności i nie tyle odpowiadać na pojawiające się problemy, co wcześniej przewidywać najważniejsze z nich, analizując ryzyko wystąpienia określonych zdarzeń, czy dopuszczenia do zaniechań, i im przeciwdziałać. Zasada ta została zawarta w przepisie art. 25 ust 1 Rozporządzenia 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, zwanego dalej *rozporządzeniem ogólnym*, które będzie miało zastosowanie w polskim porządku prawnym od dnia 25 maja 2018 r. Z powyższą zasadą ściśle związana jest zasada wyrażona w art. 25 ust. 2 rozporządzenia ogólnego, która głosi, że administrator musi wdrożyć odpowiednie środki techniczne i organizacyjne, aby domyślnie przetwarzane były wyłącznie te dane osobowe, które są niezbędne dla osiągnięcia celu przetwarzania. Warto również przytoczyć art. 35 rozporządzenia ogólnego zgodnie, z którym przed rozpoczęciem przetwarzania danych administrator danych ma obowiązek dokonać oceny skutków planowanych operacji dla ochrony danych osobowych, jeżeli dany rodzaj przetwarzania stwarza szczególne ryzyko dla praw i wolności podmiotów danych z racji swego charakteru, zakresu lub celów. Z uwagi na powyższe, już dziś dostosowując polskie prawo do ogólnego rozporządzenia należy brać pod uwagę jego przepisy.

2. Uwagi szczegółowe do założeń projektu informatycznego Platforma Integracji Usług i Danych, zagrożenia związane z projektem.

2.1. Zgodnie z Załącznikiem do uchwały nr 117/2016 Rady Ministrów z dnia 27 września 2016 r. zmieniającej uchwałę w sprawie przyjęcia programu rozwoju „Program Zintegrowanej Informatyzacji Państwa" Platforma Integracji Usług i Danych jest to narzędzie odpowiedzialne za utrzymywanie centralnego rejestru usług, techniczną integrację systemów oraz centralne monitorowanie i raportowanie dostępności usług oraz danych udostępnianych przez poszczególne systemy administracji. Z powyższej definicji wynika, że założeniem PIUiD jest scentralizowanie infrastruktury danych z rejestrów państwowych w jednym nowoutworzonym systemie oraz udostępnianie takich danych nie tylko podmiotom administracji poprzez Portal GOV.PL (tzw. konsumenci API A2A) ale również obywatelom i innym podmiotom nazywanym w projekcie konsumentami API A2B, podmiotami sektora komercyjnego czy też podmiotami sektora prywatnego. W pierwszym etapie planowane jest połączenie do PIUiD rejestrów SRP (PESEL, RDO, BUSC), CEPIK (CEP, CEK), CEIDG, ZUS oraz konsumentów API A2B w postaci banków zrzeszonych w ZBP. Kolejne etapy, zgodnie z diagramem znajdującym się w pkt 3.2 opisu założeń PIUiD *Zakres projektu – wybrane rozwiązanie wraz z uzasadnieniem* (strona 9) będą łączyć kolejne rejestry państwowe (m.in. KRS, REGON, US, KRUS, baza pełnomocnictw), poszerzać konsumentów API A2A (ZUS, CEIDG, emp@tia) oraz konsumentów komercyjnych takich jak firmy telekomunikacyjne, ubezpieczyciele, MŚP. Pkt 9.3 opisu założeń PIUiD *Analiza interesariuszy /odbiorców projektu/ beneficjentów* stanowi, że odbiorcami projektu będą w pierwszym etapie Ministerstwo Cyfryzacji, Ministerstwo Rozwoju, ZUS, dostawca brokera płatności, operator PIUiD, banki zrzeszone w ZBP.

W projekcie nie określono statusu podmiotów przetwarzających dane z punktu widzenia przepisów o ochronie danych osobowych. Tworząc system, który będzie posiadał ogromny zakres informacji o obywatelach polskich, jakim będzie PIUiD, niezbędne jest zidentyfikowanie ról poszczególnych podmiotów przetwarzających dane osobowe. Wnioskodawca powinien zatem wskazać, kto w danej sytuacji oraz w odniesieniu do jakich danych, jakich zbiorów danych występuje jako administrator danych, a kto jako podmiot przetwarzający dane w imieniu i na rzecz administratora (art. 31 u.o.d.o.). Należy ponadto jasno określić cele przetwarzania danych przez poszczególne podmioty oraz zakresy danych niezbędnych dla realizacji tych celów. Niezgodne z obowiązującym prawem byłoby udostępnienie każdemu podmiotowi z osobna pełnych informacji o konkretnych osobach z połączonych rejestrów czy to państwowych czy prywatnych. Wątpliwości GIODO w powyższej kwestii budzi w szczególności dostęp sektora prywatnego/komercyjnego do rejestrów państwowych. Z projektu założeń PIUiD nie wynika jaki jest cel i zakres takiego udostępnienia danych.

2.2. Generalny Inspektor ma na uwadze, że celem projektu PIUID jest m.in. zapewnienie interoperacyjności i transparentności rejestrów i systemów publicznych, usprawnienie procesów administracyjnych związanych ze świadczeniem usług publicznych, redukcja kosztów, uproszczenie i zinformatyzowanie procedur dostępu do informacji i danych rejestrowych, co będzie skutkowało szeroką wymianą danych osobowych. Dlatego też Generalny Inspektor wskazuje, że dostęp do tych danych powinny wyłącznie uzyskiwać podmioty uprawnione do przetwarzania takich danych dla realizacji celów wyznaczonych przepisami prawa. Zatem, ewentualne udostępnianie danych gromadzonych w systemie teleinformatycznym przeznaczonym PIUiD powinno odbywać się w trybie wnioskowym, umożliwiającym zapoznanie się jedynie z treścią sprawy wpisywaną za pomocą określonego identyfikatora, a nie ze wszystkimi danymi zgromadzonymi w systemie.

Oczywistym jest, że obywatel powinien mieć prawo dostępu tylko do danych dotyczących jego osoby. Prawa osoby, której dane dotyczą określone zostały w Rozdziale 4 u.od.o. a zgodnie z art. 32 ust. 1 u.o.d.o. zdanie pierwsze, każda osoba ma prawo do kontroli przetwarzania danych, które jej dotyczą, zawartych w zbiorach danych a administrator danych ma obowiązek je zabezpieczać również poprzez odpowiednią weryfikację tożsamości obywatela przy użyciu dostępnych środków identyfikacji elektronicznej.

Tworzenie kanałów udostępniania informacji dla administracji i podmiotów sektora prywatnego, za pośrednictwem których będzie można pozyskiwać informacje z różnych rejestrów państwowych i komercyjnych może w konsekwencji prowadzić do nadużyć, polegających na pozyskiwaniu niekontrolowanej ilości danych o obywatelach przez urzędników lub pracowników podmiotów sektora prywatnego dysponujących takim narzędziem dla swoich celów. Innym zagrożeniem jest potencjalne wykorzystanie takiej platformy do dowolnego profilowania osób przez administrację lub podmioty komercyjne poprzez odpowiednie zestawienie różnych informacji pozyskanych z udostępnianych rejestrów, w szczególności do analizy lub prognozy aspektów dotyczących efektów pracy tej osoby fizycznej, jej sytuacji ekonomicznej, zdrowia, osobistych preferencji, zainteresowań, wiarygodności, zachowania, lokalizacji lub przemieszczania się. GIODO zauważa, że w projekcie brak jest szczegółowych informacji w zakresie dotyczącym warunków uzyskiwania dostępów do powstałych w ramach projektu (Application Programming Interface) API oraz zakresu pozyskiwanych danych.

Jednocześnie należy zauważyć, że PIUiD – jako system umożliwiający centralizację dostępu do danych z rejestrów państwowych i komercyjnych – może stać się łatwym celem ataków hakerów i crakerów, którzy w przypadku udanego włamania do

PIUiD będą mieli dostęp do danych o obywatelach ze wszystkich połączonych rejestrów. Oczywistym jest, że zdobyte w ten sposób dane z różnych rejestrów powiązane ze sobą mogą być wykorzystane dla celów przestępczych.

Podsumowując powyższe uwagi Generalny Inspektor Ochrony danych Osobowych wnioskuje o wstrzymanie prac technicznych prowadzących do uruchomienia PIUiD do chwili ustalenia odpowiednich przepisów prawa, które będą regulować ramy prawne jego działania. Zgodzić się należy, iż państwo powinno dążyć do zwiększania zaufania obywateli do państwa i stanowionego przez nie prawa co przyświeca zasadzie demokratycznego państwa prawnego urzeczywistniającego zasady sprawiedliwości społecznej. Jednak wprowadzanie ułatwień dla obywateli w uzyskiwaniu informacji o wykorzystywaniu danych ich dotyczących musi się odbywać z poszanowaniem zasad ochrony danych osobowych. Tylko wówczas planowane rozwiązania będą mogły funkcjonować w sposób zgodny z prawem. Jasne i przejrzyste rozpisanie zasad przetwarzania danych osobowych jest niezbędne, aby osoby, których dane te dotyczą miały świadomość, kto, w jakim zakresie, w jaki sposób, w jakich celach oraz przez jaki okres przetwarza dotyczące ich informacje. Zapewni to wzrost zaufania obywateli do państwa, co jest warunkiem efektywnego i bezproblemowego wdrożenia projektowanych rozwiązań.

GIODO pragnie również podkreślić, że zamieszczenie wskazanych w niniejszym piśmie informacji jest warunkiem niezbędnym do zapewnienia projektowi zgodności z przepisami obowiązującego prawa w zakresie ochrony danych osobowych. Celem zgłaszanych uwag jest wsparcie projektodawcy w zapewnieniu zgodności projektowanej regulacji z obowiązującymi przepisami, jak również wskazanie, iż brak przejrzystych regulacji dotyczących zakresu przetwarzanych danych osobowych osób fizycznych, kompetencji organów objętych zakresem projektowanej regulacji, jak również informacji pozwalających na weryfikację prawidłowości stosowanych przez te podmioty zasad przetwarzania skutkować będzie wnoszeniem przez osoby fizyczne skarg na nieprawidłowości związane z przetwarzaniem danych osobowych. GIODO wskazuje, że w odniesieniu do ochrony danych osobowych ważne jest wprowadzenie takich rozwiązań kształtujących prawa jednostki, które będą formułować przepisy w sposób jasny, precyzyjny i zupełny oraz będą określać zasady przetwarzania danych osobowych w taki sposób, by podmioty – w tym z sektora publicznego – stosujące je w przyszłości, mogły opierać na jasnej podstawie prawnej swoje działania. Takie działanie sprawi, iż stosowanie takich przepisów przez administratorów danych osobowych nie będzie problematyczne.

Jednocześnie GIODO stwierdza, że powinna nastąpić szersza dyskusja przede wszystkim na temat przepisów prawa, które miałyby regulować projektowane rozwiązania, jak również uwzględniających zasady przetwarzania danych osobowych. Za niewystarczające uznać należy planowane oddanie uregulowania tych zasad mocą porozumień pomiędzy ministrem właściwym do spraw informatyzacji a organami prowadzącymi rejestry publiczne, czy podmiotami sektora

prywatnego wykorzystującymi własne rejestry. Generalny Inspektor będzie włączał się aktywnie w prace nad projektem przepisów prawa dotyczących PIUiD przedstawiając wówczas stosowne uwagi i postulaty celem wypracowania właściwych przepisów prawa w tym zakresie z uwzględnieniem zasad przetwarzania danych osobowych.