GENERALNY INSPEKTOR OCHRONY DANYCH OSOBOWYCH

dr Edyta Bielak-Jomaa

Warszawa, dnia 21 czerwca 2016 r.

DOLiS-033-225/16/KK

Pani
Anna Streżyńska
Minister Cyfryzacji
ul. Królewska 27
00-060 Warszawa

w odpowiedzi na pismo z dnia […] czerwca 2016 r. (znak: […]) dotyczące:

1) projektu **rozporządzenia w sprawie zakresu i warunków korzystania z elektronicznej platformy usług administracji publicznej** wydawanego na podstawie delegacji zawartej w art. 19a ust. 3 ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz. U. z 2014 r. poz. 1114 z późn. zm.);

2) projektu **rozporządzenia w sprawie zasad i warunków potwierdzania, przedłużania ważności, unieważniania oraz wykorzystywania profilu zaufanego elektronicznej platformy usług administracji publicznej** wydawanego na podstawie delegacji zawartej w art. 20a ust. 3 ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz. U. z 2014 r. poz. 1114 z późn. zm.);

uprzejmie informuję, iż **Generalny Inspektor Ochrony Danych Osobowych** – z punktu widzenia przepisów ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2015 r. poz. 2135, z późn. zm.) – **zgłasza następujące uwagi**.

Ad 1)

W § 3 ust. 1 projektu proponuje się rozszerzenie zakresu danych wymaganych do założenia konta przez użytkownika. W ocenie organu do spraw ochrony danych osobowych nie jest uzasadnione rozszerzenie katalogu danych osobowych pozyskiwanych dla tego celu, skoro w

obowiązującym stanie prawnym projektodawca za wystarczające do założenia konta uznał podanie imienia, nazwiska, adresu poczty elektronicznej oraz identyfikatora użytkownika.

Projektowany przepis poszerza wskazany wyżej zakres danych o numer PESEL (§ 3 ust. 1 pkt 3) oraz numer telefonu komórkowego (§ 3 ust. 1 pkt 5). W uzasadnieniu projektu wskazano, iż pozyskiwanie numeru PESEL jest związane z planami połączenia procedur zakładania konta w systemie ePUAP oraz składania wniosku o potwierdzenie profil zaufanego ePUAP. Należy zauważyć, iż organ ochrony danych osobowych wielokrotnie podnosił zastrzeżenia w odniesieniu do zasad posługiwania się profilem zaufanym użytkownika na Platformie ePUAP, które wiąże się z koniecznością ujawniania numeru PESEL.[1] Generalny Inspektor podkreślał, że udogodnienia oparte na identyfikacji osób w systemach e-goverment, zarówno w odniesieniu do urzędników, jak i innych osób np. przy rejestracji działalnosci gospodarczej, nie mogą następować kosztem naruszenia konstytucyjnie chronionych praw i wolności. Zastosowanie numeru PESEL może naruszyć prywatność danych osobowych obywatela poprzez możliwość powiązania z innymi rejestrami oraz z uwagi na semantyczność cech tego identyfikatora (data urodzenia i płeć). Należy również pamiętać, że na podstawie prawa do ponownego wykorzystania informacji publicznej będzie można przetwarzać taką informację w dowolnym komercyjnym lub niekomercyjnym celu. Ponadto za pomocą numeru PESEL znacznie ułatwione jest „profilowanie" użytkownika Internetu. Stąd w opinii Generalnego Inspektora konieczne jest rzetelne rozważenie zagadnienia zakresu danych wykorzystywanych w powyższych sytuacjach, z uwzględnieniem zasady adekwatności danych, a zatem ograniczenia zakresu danych do niezbędnego dla realizacji ściśle określonego celu (art. 26 ust. 1 pkt 3 ustawy). **Należy poszukiwać innych efektywnych rozwiązań w tym zakresie - np. wykorzystywanie w tym celu innego rodzaju numeru pozwalającego na uwierzytelnianie ważności certyfikatu i tożsamości osoby podpisującej się podpisem elektronicznym, przy zastosowaniu rozwiązania, że szerszy zestaw danych osobowych, w tym numer PESEL, byłby dostępny do wiadomości podmiotu świadczącego usługi certyfikacyjne.**

W związku z powyższym do Biura Generalnego Inspektora trafia coraz więcej sygnałów osób zaniepokojonych udostępnianiem numeru PESEL w związku z korzystaniem z ePUAP i profilu zaufanego. Pracownicy organów kontrolnych muszą udostępniać swój podstawowy identyfikator osobom, wobec których prowadzą postępowania. Obawę budzi możliwość jego wykorzystania w sposób nieprawidłowy przez odbiorców korespondencji elektronicznej. W związku z powyższym, organ do spraw ochrony danych osobowych tym bardziej sprzeciwia się, by udostępnianie numeru PESEL było obowiązkowe już na etapie zakładania konta dla użytkownika.

[1] Ostatnio w toku prac Ministerstwa Rozwoju nad projektem ustawy o usługach zaufania, identyfikacji elektronicznej oraz zmianie niektórych ustaw (DOLiS-033-92/16 oraz DOLiS-072-24/13). Pismo z uzgodnień międzyresortowych: DOLiS-033-92/16/KK/27913 - http://legislacja.rcl.gov.pl/docs//2/12283556/12343431/12343434/dokument216731.pdf

Generalny Inspektor ma wątpliwości co do konieczności podawania numeru telefonu komórkowego w celu założenia konta. Nie kwestionując fakultatywności podawania tej danej (przez osoby, które chcą otrzymywać informacje z systemu na numer telefonu komórkowego), nie można jednocześnie wyrazić aprobaty wobec jej wymuszania poprzez wprowadzenie obowiązku jej udostępnienia. Obligatoryjne podawanie numeru telefonu komórkowego spowodowałoby, iż założenie konta dla użytkownika w systemie ePUAP byłoby dostępne wyłącznie dla osób, które taki numer posiadają (a tym samym ograniczałoby dostęp obywateli do usług administracji publicznej realizowanych drogą elektroniczną). Powyższe pozostaje wątpliwe, albowiem w polskim porządku prawnym nie istnieje obowiązek posiadania telefonu komórkowego. Takiego obowiązku nie powinny nakładać komentowane przepisy. Dlatego zawsze, gdy przepisy miałyby przewidywać udostępnianie numeru telefonu komórkowego, czynność ta powinna być traktowana jako fakultatywna. Przeciwdziałałoby to procesowi wykluczania cyfrowego osób niekorzystających z różnych przyczyn ze wszystkich środków komunikacji elektronicznej.

Od 1 maja 2008 roku, ustawa z dnia 17 lutego 2005 roku o informatyzacji działalności podmiotów realizujących zadania publiczne, nakłada na wszystkie urzędy administracji publicznej obowiązek obsługi interesantów drogą elektroniczną z wykorzystaniem podpisu elektronicznego. Tym samym, w świetle obowiązujących przepisów ustawowych, nie jest dopuszczalne uzależnianie możliwości korzystania z usług administracji publicznej drogą elektroniczną od spełnienia dodatkowych warunków, takich jak posiadanie telefonu komórkowego. Tego rodzaju ograniczeń nie powinny zwłaszcza nakładać przepisy aktu o randze niższej niż ustawa.

W § 3 ust. 7 proponuje się, by „W przypadku utraty identyfikatora użytkownika lub hasła, o których mowa w ust. 2 pkt 1, użytkownik może wnioskować, za pośrednictwem ePUAP, o przesłanie na adres poczty elektronicznej użytkownika, o którym mowa w ust. 1 pkt 4, odpowiednio identyfikatora użytkownika albo hasła tymczasowego. Użytkownik po uwierzytelnieniu się za pomocą hasła tymczasowego określa nowe hasło, którego stopień złożoności kontroluje ePUAP". Przepis powyższy zakłada pełne bezpieczeństwo poczty elektronicznej, w tym zapewnienie poufności przekazywanej informacji podczas jej przekazywania, co jest założeniem zbyt ryzykownym, biorąc pod uwagę kategorię świadczonych usług. Powszechnie wiadomo jednak, że standardowe usługi poczty elektronicznej nie zapewniają poufności przekazywanych informacji. Ponadto dostęp użytkownika do jego poczty nie zawsze jest właściwie zabezpieczany przez samych użytkowników. Możliwym jest rozważenie dodatkowych zabezpieczeń przekazywanego hasła tymczasowego poprzez np. jego zakodowanie, kluczem który przekazywany byłby innym kanałem komunikacji np. SMS-em na numer telefonu komórkowego użytkownika. **W takim wypadku przetwarzanie danych o numerze telefonu byłoby uzasadnione. W obecnym brzmieniu nie wskazano uzasadnienia dla przetwarzania informacji**

o numerze. W związku z tym powyżej poczynione uwagi co do niezbędności przetwarzania numeru PESEL mają odpowiednie zastosowanie.

W § 5 ust. 2 pkt 3 wymaga się, by wniosek zawierał dane administratora podmiotu. Jednocześnie nie wskazano, jakie dane miałyby być podawane. Celem uniknięcia podawania szerokiego katalogu danych przez podmioty wnioskujące, proponuje się jego wyczerpujące określenie.

W § 10 ust. 1 zaproponowano: „Platforma ePUAP może wymieniać informacje z innymi systemami teleinformatycznymi podmiotów określonych w art. 2 ust. 1 i 2, w **art. 19c ust. 1** ustawy oraz podmiotów niepublicznych". Mając na uwadze fakt, że **art. 19c ust 1 ustawy** wskazuje podmioty, o których mowa w art. 2 ust. 3 ustawy. Cały zapis zawarty w § 10 ust. 1 projektu można by skrócić do postaci: „Platforma ePUAP może wymieniać informacje z innymi systemami teleinformatycznymi podmiotów określonych w art. 2 ust. 1, 2 i 3 ustawy oraz podmiotów niepublicznych". Przeredagowanie § 10 ust 1 w powyższy sposób nie zmieni jego znaczenia upraszczając formę przekazu.

Ad 2)

W § 9 ust. 1 pkt 3 projektu wskazano, iż profil zaufany zawiera numer PESEL użytkownika. Uwagi poczynione wyżej w tym zakresie mają także tutaj zastosowanie. Numer PESEL nie powinien być widoczny dla odbiorców korespondencji, tak by nie mógł być przez nich wykorzystywany w innych celach.

W § 9 ust. 1 pkt 9 projektu przewidziano rozwiązanie polegające na obligatoryjnym podawaniu numeru telefonu komórkowego jako jednego z elementów profilu zaufanego ePUAP. W przypadku akceptacji proponowanego przez projektodawcę rozwiązania będzie to oznaczało, że osoby nieposiadające telefonu komórkowego nie będą mogły utworzyć profilu zaufanego, co w znaczący sposób ogranicza możliwość dostępu do profilu zaufanego ePUAP, jak również ogranicza możliwość autoryzacji. W opinii Generalnego Inspektora, sposób autoryzacji powinien następować – według wyboru użytkownika – na adres poczty elektronicznej lub numer telefonu komórkowego.

Uwagę Generalnego Inspektora przyciągnęło niedoprecyzowanie odpowiedzialności za czynności materialne i prawne zrealizowane na skutek użyciu nieważnego profilu zaufanego ePUAP. **W § 13 projektu** wskazano jedynie, że „Profil zaufany ePUAP potwierdzony na podstawie nieprawdziwych lub nieaktualnych danych jest nieważny od dnia jego potwierdzenia". Nie została natomiast uregulowana sprawa odpowiedzialności za skutki niewłaściwej weryfikacji danych właściciela konta profilu zaufanego skutkujące potwierdzeniem profilu zaufanego na podstawie sfałszowanych dokumentów lub celowo dokonanego oszustwa.