



**GENERALNY INSPEKTOR
OCHRONY DANYCH
OSOBOWYCH**

dr Edyta Bielak-Jomaa

Warszawa, dnia 16 maja 2016 r.

DOLiS-033-135/16

Pan
Marcin Warchol
Podsekretarz Stanu
w Ministerstwie Sprawiedliwości
al. Ujazdowskie 11,
00-950 Warszawa

w nawiązaniu do pisma z dnia [...] kwietnia 2016 roku dotyczącego projektu **rozporządzenia Ministra Sprawiedliwości w sprawie sposobu przeprowadzenia licytacji elektronicznej** [wydawanego na podstawie delegacji zawartej w art. 879¹¹ ustawy z dnia 17 listopada 1964 r. – Kodeks postępowania cywilnego (Dz. U. z 2014 r. poz. 101, z późn. zm.), (zwanego dalej projektem.)] uprzejmie informuję, że Generalny Inspektor Ochrony Danych Osobowych – z punktu widzenia przepisów ustawy z dnia 29 sierpnia 1997 roku o ochronie danych osobowych (Dz. U. z 2015 r. poz. 2135, z późn. zm.), (zwanej dalej *ustawą o ochronie danych osobowych*) – zgłasza następujące uwagi.

- Generalny Inspektor Ochrony Danych Osobowych **zgłasza uwagę ogólną do tytułu projektu rozporządzenia**, w którym użyto sformułowania „w sprawie sposobu przeprowadzenia licytacji elektronicznej”. Biorąc pod uwagę, iż licytacja elektroniczna, jako sposób przeprowadzania zakupu lub sprzedaży, znajduje zastosowanie w wielu różnych instytucjach (np. w postępowaniach o zamówienia publiczne albo prywatnie np. przez portal Allegro.pl), należałoby dokonać modyfikacji tytułu projektu rozporządzenia, tak by

przedmiot regulacji nie wzbudzał wątpliwości. W związku z powyższym, organ do spraw ochrony danych osobowych sugeruje by do tytułu projektu rozporządzenia po słowach „w sprawie sposobu przeprowadzenia licytacji elektronicznej” dodać słowa „przez komornika”.

- **Zastrzeżenia budzi § 7 ust. 1 pkt 1 projektu**, w którym wskazano katalog zamknięty danych osobowych zawartych we wniosku o założenie konta użytkownika w systemie teleinformatycznym. Wskazano, iż wymagany jest m.in. numer PESEL, o ile został osobie nadany, oraz numer dokumentu tożsamości, a także wskazanie miejsca urodzenia. Natomiast w § 7 ust. 4 projektu wskazano, iż automatycznej weryfikacji w zbiorze PESEL podlega imię i nazwisko oraz numer PESEL. Mając na uwadze powyższe, zbędnym jest zawieranie we wniosku przez osoby posiadające numer PESEL dodatkowych danych z dokumentu tożsamości, jak i podania miejsca urodzenia. Dodatkowe dane powinny być podawane dopiero w przypadku negatywnego wyniku weryfikacji z ww. systemu (§ 7 ust. 5 projektu) lub w przypadku osób, które nie posiadają numeru PESEL i zgłaszają operatorowi wniosek, za pośrednictwem wybranego komornika sądowego (§ 7 ust. 2 projektu).

Zawieranie danych dodatkowych we wniosku, w przypadku osób posiadających numer PESEL, godzi w zasadę adekwatności zawartą w art. 26 ust. 1 pkt 3 ustawy o ochronie danych osobowych, która wymaga, aby zbierane dane były adekwatne do celów, w jakich są przetwarzane. Rodzajem i treścią dane nie powinny wykraczać poza potrzeby wynikające z celu ich zbierania. Względem powyższą zasadę przemawia przeciwko zbieraniu zarówno wszelkich danych dla danego celu nieistotnych, niemających znaczenia, jak i danych o „większej szczegółowości”. Wskazanie przez wnioskodawcę, posiadającego numer PESEL, numer dokumentu tożsamości oraz miejsce urodzenia jest w niniejszym przypadku zbędne. Powyższe rozwiązanie znajdowałoby odzwierciedlenie w przypadku osób, które numeru PESEL nie posiadają. Wtedy konieczne byłoby podanie w zamian numeru dokumentu tożsamości oraz miejsca urodzenia.

W związku z powyższym Generalny Inspektor wskazuje, iż zasadnym byłoby doprecyzowanie § 7 ust. 1 pkt 1 projektu poprzez zamieszczenie między słowami „imiona i nazwisko wnioskodawcy”, a „adresu poczty elektronicznej oraz adresu do korespondencji”, słów: „numer PESEL, a w przypadku osoby nieposiadającej numeru PESEL - serię, numer i nazwę dokumentu potwierdzającego tożsamość oraz nazwę państwa, które wydało ten dokument”.

Dodatkowo projektodawca w § 7 ust. 2 projektu niekonsekwentnie przyjmuje rozróżnienie między osobami posiadającymi numer PESEL, a tymi które go nie posiadają. W związku z powyższym stanowi to dodatkowy argument do tego, by w § 7 ust. 1 pkt 1 projektu również to rozróżnienie zawrzeć.

- **Odnosząc się do § 7 ust. 6 projektu**, zastrzeżenia budzi sposób przekazywania danych uwierzytelniających, który należy uznać za niespełniający wymaganych warunków bezpieczeństwa. Dane umożliwiające uwierzytelnienie konta w systemie teleinformatycznym (tj. login i hasło) są przekazywane wnioskodawcy za pośrednictwem medium, które nie zapewnia wystarczającej poufności. Generalny Inspektor Ochrony Danych Osobowych wskazuje, iż sposób ten jest niezgodny z zaleceniem nr 2 rekomendacji MAC/SEC/1/15 wydanym przez Ministra Cyfryzacji w kwietniu 2015 roku, którego celem jest zapewnienie integralności i autentyczności korespondencji elektronicznej przesyłanej pomiędzy podmiotami publicznymi, jak również kierowanej do podmiotów zewnętrznych i obywateli.

Dodatkowo w § 7 ust. 6 projektu wskazano, iż „osobę składającą wniosek zawiadamia się o założeniu konta w systemie teleinformatycznym. W zawiadomieniu podaje się login i hasło użytkownika”. Natomiast w **§ 9 ust. 2 pkt 2 projektu** wskazano, iż „wniosek, poza danymi, o których mowa w § 7, zawiera: nazwę użytkownika”. Generalny Inspektor prosi o wyjaśnienie, w jaki sposób należy rozumieć w niniejszym przypadku „nazwę użytkownika” (§ 9 ust. 2 pkt 2 projektu). W szczególności, czy pojęcie to jest tożsame z pojęciem „login” użytym w § 7 ust. 6 projektu? Organ do spraw ochrony danych osobowych wskazuje, iż żadne z powyższych pojęć nie zostało przez projektodawcę zdefiniowane.

- W § 3 projektu wskazano, iż „operator weryfikuje dane komornika zakładającego konto w systemie teleinformatycznym i zawiadamia go za pośrednictwem poczty elektronicznej o danych umożliwiających uwierzytelnienie się na koncie”. Natomiast w **§ 17 projektu rozporządzenia** wskazano, iż „operator w terminie 14 dni od daty wejścia w życie niniejszego rozporządzenia zawiadamia komorników o założeniu kont w systemie teleinformatycznym oraz udostępnia każdemu komornikowi login i hasło umożliwiające uwierzytelnienie się na koncie”. Interpretując § 17 projektu rozporządzenia, bez wzięcia pod uwagę § 3 projektu, można przypuszczać, iż operator zakłada komornikom konta

w systemie teleinformatycznym z urzędu, a nie na wniosek (jak zostało to wskazane w § 3 projektu). Natomiast w sytuacji odwrotnej, tj. biorąc pod uwagę § 3 projektu, można przypuszczać, iż dane weryfikujące komornika zakładającego konto na wniosek, są przekazywane bezpośrednio po jego założeniu. Generalny Inspektor Ochrony Danych Osobowych wskazuje, iż ww. przepisy wymagają uspoźnienia, tak by nie wprowadzały w błąd i nie powodowały błędnej interpretacji.

- W treści projektu rozporządzenia przyjmuje się, iż komornicy przy korzystaniu z systemu teleinformatycznego uwierzytelniać się będą wyłącznie poprzez użycie login-u i hasła (**§ 17 projektu rozporządzenia**). Mając na uwadze powyższe, zarówno urzędnik państwowy, jak i osoby prywatne do uwierzytelnienia konta w systemie teleinformatycznym stosują wyłącznie login i hasło. Organ do spraw ochrony danych osobowych zwraca uwagę, iż taka praktyka jest niezgodna z zaleceniem nr 1 rekomendacji MAC/SEC/1/15 wydanym przez Ministra Cyfryzacji w kwietniu 2015 roku, która zaleca wzmocnienie mechanizmów uwierzytelniania stosowanych w systemach back office podmiotów realizujących zadania publiczne.
- dodatkowo Generalny Inspektor wskazuje, iż w **§ 9 ust. 2 projektu** występuje techniczny błąd legislacyjny, gdyż katalog danych, o których mowa w ww. projektowanym przepisie znajduje się w § 7 ust. 1 projektu, a nie jak ogólnie wskazano w § 7 projektu.

Jednocześnie informuję, iż przedstawiony projekt ustawy pozostaje przedmiotem zainteresowania organu do spraw ochrony danych osobowych, dlatego też Generalny Inspektor Ochrony Danych Osobowych zastrzega sobie prawo do zgłaszania uwag na dalszych etapach prac legislacyjnych.