GENERALNY INSPEKTOR OCHRONY DANYCH OSOBOWYCH

dr Edyta Bielak-Jomaa

Warszawa, dnia 4 maja 2017 r.

DOLIS-023-153/17

Pan
Adam Podgórski
Zastępca Szefa Kancelarii Sejmu
ul. Wiejska 4/6/8
00 – 902 Warszawa

w odpowiedzi na pismo z dnia 5 kwietnia 2017 r. informuję, iż do poselskiego projektu Klubu Poselskiego Nowoczesna ***ustawy o zmianie ustawy o samorządzie gminnym oraz niektórych innych ustaw*** Generalny Inspektor Ochrony Danych Osobowych - z punktu widzenia przepisów ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz.U. z 2016 r., poz.922)- **zgłasza następujące uwagi.**

Przewidziana w projekcie ustawy możliwość występowania z inicjatywą uchwałodawczą mieszkańców gmin, powiatów i województw będzie wiązała się z przetwarzaniem danych osobowych osób tworzących komitet inicjatywy uchwałodawczej a także danych osobowych mieszkańców składających podpisy pod projektami określonych uchwał.

W przedmiotowym projekcie brak jest przepisów, które określałyby kto miałby być administratorem danych osobowych (podmiotem decydującym o celach i środkach przetwarzania danych osobowych, o którym mówi art. 7 pkt 4 ustawy o ochronie danych osobowych), pozyskiwanych w wykazach podpisów mieszkańców gmin, powiatów i województw. Na podobny problem Generalny Inspektor Ochrony Danych Osobowych zwrócił już uwagę w odniesieniu do ustawy z dnia 24 czerwca 1999 r. o wykonywaniu inicjatywy ustawodawczej przez obywateli

ul. Stawki 2, 00-193 Warszawa
tel. 22 531-04-40
fax 22 531-04-41
www.giodo.gov.pl

(Dz.U. 1999 r., poz. 62 Nr 688), kierując wystąpienie o wprowadzenie właściwych regulacji do powyższej ustawy do Ministerstwa Spraw Wewnętrznych i Administracji [1].

W przedmiotowym wystąpieniu GIODO wskazał, iż w ustawie o wykonywaniu inicjatywy ustawodawczej nie zostało wskazane, kto odpowiada za ochronę danych osobowych zgromadzonych w toku zbierania podpisów pod konkretnym projektem obywatelskim, kto jest ich administratorem, w tym także w sytuacji, kiedy dany komitet inicjatywy ustawodawczy ulegnie rozwiązaniu.

Analogiczny problem stanowić może brak odpowiednich regulacji w opiniowanym projekcie ustawy.

Zgodnie z art. 23 ust.1 ustawy ochronie danych osobowych przetwarzanie danych jest dopuszczalne tylko wtedy, gdy 1) osoba, której dane dotyczą wyrazi na to zgodę, chyba, że chodzi o usunięcie dotyczących jej danych; 2) jest to niezbędne dla zrealizowania uprawnienia lub spełnienia obowiązku wynikającego z przepisu prawa; 3) jest to konieczne do realizacji umowy, gdy osoba, której dane dotyczą, jest jej stroną lub gdy jest to niezbędne do podjęcia działań przed zawarciem umowy na żądanie osoby, której dane dotyczą 4) jest to niezbędne do wykonania określonych prawem zadań realizowanych dla dobra publicznego; 5) jest to niezbędne dla wypełnienia prawnie usprawiedliwionych celów realizowanych przez administratorów danych albo odbiorców danych, a przetwarzanie nie narusza praw i wolności osoby, której dane dotyczą. Zatem, zgodnie z ust. 2 powołanego artykułu przetwarzanie danych osobowych powinno znaleźć oparcie w powszechnie obowiązujących przepisach prawa, w tym przypadku – ustawie o zmianie ustawy o samorządzie gminnym oraz niektórych innych ustaw.

Obowiązki administratora danych zostały określone w art. 26 ust.1 ustawy o ochronie danych osobowych. W myśl wskazanego przepisu administrator danych przetwarzający dane osobowe, powinien dołożyć szczególnej staranności w celu ochrony interesów osób, których dane dotyczą, w szczególności jest zobowiązany zapewnić, by dane te były: 1) przetwarzane zgodnie z prawem, 2) zbierane dla oznaczonych, zgodnych z prawem celów i niepoddawane dalszemu przetwarzaniu niezgodnemu z tymi celami, z zastrzeżeniem ust.2; 3) merytorycznie poprawne i adekwatne w stosunku do celów, w jakich są przetwarzane; 4) przechowywane w postaci umożliwiającej identyfikację osób, których dotyczą, nie dłużej niż jest to niezbędne do osiągniecia celu przetwarzania. Po osiągnięciu celu dane powinny zostać usunięte o ile ich dalsze przetwarzanie nie jest dopuszczalne na podstawie stosownych przepisów prawa. Zgodnie z art. 26 ust. 2 ustawy o ochronie danych osobowych przetwarzanie danych osobowych w celu innym niż ten, dla którego zostały zebrane, jest dopuszczalne, jeżeli nie narusza praw i wolności osoby, której dane dotyczą,

[1] DOLIS-035-2106/16/AG, Ministerstwo Spraw Wewnętrznych i Administracji przekazało sprawę wg właściwości Ministerstwu Cyfryzacji.

oraz następuje w celach badań naukowych, dydaktycznych, historycznych lub statystycznych i z zachowaniem przepisów art. 23 i 25 ustawy. Ponadto, na podstawie art. 36 ust. 1 ustawy, administrator danych jest zobowiązany zastosować środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych odpowiednią do zagrożeń oraz kategorii danych objętych ochroną, a w szczególności powinien zabezpieczyć dane przed ich udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ustawy oraz zmianą, utratą, uszkodzeniem lub zniszczeniem.

Podsumowując, projektodawca powinien określić podmiot odpowiedzialny za przestrzeganie wyżej wymienionych zasad. Nie jest bowiem oczywiste, że to komitet inicjatywy uchwałodawczej miałby być administratorem danych osobowych gromadzonych w toku zbierania podpisów pod określonymi projektami inicjatywy uchwałodawczej. Zakładając jednak, że tak miałoby być, wątpliwości budzi kwestia, kto miałby odpowiadać za listy z podpisami zgromadzonymi przez komitet inicjatywy ustawodawczej od momentu przekazania ich przewodniczącemu rady gminy, rady powiatu i sejmiku województwa, albo w sytuacji, gdy dany komitet ulegnie rozwiązaniu.

Przepisy ustawy nie muszą wprost wskazywać, kto jest administratorem danych określonego zbioru danych, o ile będą określać cały proces inicjatywy uchwałodawczej, by znane były jej poszczególne etapy i towarzyszący im proces przetwarzania danych osobowych osób popierających dany projekt. Ustawodawca powinien precyzować jakie są cele przetwarzania danych osobowych oraz sposoby ich wykorzystywania, tak by regulacja była wyczerpująca dla realizacji celów ustawy, ale i bezpieczeństwa danych.

Generalny Inspektor Ochrony Danych Osobowych zwraca również uwagę na przepisy 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 (ogólne rozporządzenie o ochronie danych), Dz.U. L 119 z 4.5.2016, s. 1; dalej zwane: RODO, które nakłada na podmioty, które biorą udział w procesie przetwarzania danych osobowych, wiele nowych obowiązków i uprawnień.

Wśród nich znalazł się obowiązek uwzględnienia ochrony danych w fazie projektowania (*privacy by design*). Zgodnie z art. 25 ogólnego rozporządzenia: „uwzględniając stan wiedzy technicznej, koszt wdrożenia oraz charakter, zakres, kontekst i cel przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie wystąpienia i wadze zagrożenia 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 spełniać wymogi niniejszego rozporządzenia oraz chronić prawa osób, których dane dotyczą".

Rozporządzenie ogólnym o ochronie danych osobowych będzie miało zastosowanie w polskim porządku prawnym od dnia 25 maja 2018 r. zatem, już dziś dostosowując polskie prawo do ogólnego rozporządzenia należy brać pod uwagę jego przepisy.

Odnosząc się do proponowanych zapisów projektu, Generalny Inspektor zwraca uwagę na zakres danych osobowych, które miałyby być zamieszczane w pisemnym oświadczeniu o przystąpieniu do komitetu inicjatywy uchwałodawczej w zmienianych projektem trzech ustawach: o samorządzie gminnym; o samorządzie powiatowym; o samorządzie województwa. Wątpliwości Generalnego Inspektora Ochrony Danych Osobowych budzi konieczność podawania w oświadczeniach adresu zamieszkania założycieli komitetu. Jeżeli adres miałby być pozyskiwany w celu weryfikacji czy dana osoba jest faktycznie mieszkańcem danej gminy, powiatu, województwa, rozważyć należy, czy w tym wypadku nie byłby wystarczający obowiązek podawania np. kodu pocztowego lub miejscowości, co również potwierdziłoby, iż dana osoba jest rzeczywiście mieszkańcem danej gminy, powiatu, województwa. W tym samym zakresie Generalny Inspektor zgłasza zastrzeżenia co do konieczności podawania adresu zamieszkania w zawiadomieniu o utworzeniu komitetu do przewodniczącego rady gminy, przewodniczącego rady powiatu i przewodniczącego sejmiku województwa.

W projekcie ustawy nie określono jakie dane osobowe będzie zawierał wykaz podpisów mieszkańców gmin, powiatów, województw. Przepisy prawa powinny wskazywać zakres danych jakie konkretnie miałyby się znajdować w przedmiotowych wykazie i tym samy stanowić katalog zamknięty.

Niedoprecyzowanie jak szczegółowe będą to informacje może prowadzić do dowolności interpretacyjnej tak sformułowanego przepisu i pozyskiwania różnych, innych informacji niekoniecznie bezpośrednio związanych z celem ich przetwarzania a w konsekwencji zbędnych, nieadekwatnych, „na zapas". Taka konstrukcja przedmiotowego przepisu jest w ocenie GIODO niezgodna z zasadami legalizmu, celowości i adekwatności, (wynikającymi z przytoczonego wyżej art. 26 ust. 1 pkt 1 – 3 ustawy o ochronie danych osobowych), które projektodawca powinien brać pod uwagę tworząc rozwiązania prawne związane z przetwarzaniem danych osobowych.

Generalny Inspektor Ochrony Danych Osobowych wskazuje na powyższe, celem wzięcia pod uwagę przez projektodawcę, że ważne jest formułowanie przepisów prawa w taki sposób, by podmioty stosujące je w przyszłości, mogły swe działania na danych osobowych opierać na jasnej podstawie prawnej. To z przepisów prawa powinno w sposób wyczerpujących wynikać jakie, dokumenty lub/i informacje są niezbędne i proporcjonalne do celów jakie mają być mocą tych przepisów realizowane. Rolą ustawodawcy jest natomiast wyważenie i precyzyjne wskazanie rozwiązań pozwalających osiągnąć określone przepisami cele z użyciem środków czy rozwiązań, jak najmniej ingerujących w autonomię informacyjną jednostki, której dane mogą być przetwarzane.