GENERALNY INSPEKTOR OCHRONY DANYCH OSOBOWYCH

dr Edyta Bielak-Jomaa

Warszawa, dnia 8 kwietnia 2016 r.

DOLiS-033-92/16/KK

Podsekretarz Stanu
w Ministerstwie Rozwoju

w odpowiedzi na pismo z dnia 22 marca br. o sygn. NK:62658/2016 (data wpływu do Biura GIODO: 4 kwietnia br.) dot. **projektu ustawy o usługach zaufania, identyfikacji elektronicznej oraz zmianie niektórych ustaw** (**zwanego dalej projektem**) 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., **zwanej dalej ustawą**) – **zgłasza następujące uwagi**.

W **art. 4 ust. 3 projektu** wskazano, iż nadzór w odniesieniu do niekwalifikowanych dostawców jest realizowany w przypadku wystąpienia znaczących incydentów związanych z bezpieczeństwem lub utratą integralności, jeżeli poważnie zagrożony może zostać interes odbiorców usług zaufania. W opinii Generalnego Inspektora jest to zawężenie sprzeczne z intencjami rozporządzenia eIDAS[1] wyrażonymi w motywie nr 36, w którym wskazano, że organ nadzoru powinien podejmować działania, gdy został poinformowany, że niekwalifikowany dostawca usług zaufania nie spełnia wymogów niniejszego rozporządzenia. Nie istnieje racjonalne uzasadnienie dla w/w proponowanego ograniczenia zakresu nadzoru, w sytuacji przetwarzania danych osobowych usługobiorców i innych podmiotów w stosunku do kwalifikowanych dostawców.

W **art. 21 ust. 1 pkt 2 projektu** proponuje się wpisywanie do rejestru kwalifikowanej usługi zaufania. Może to kolidować z przepisem art. 20 ust. 2 projektu, w którym wskazano cele prowadzenia rejestru (ewidencjowanie dostawców usług zaufania oraz udostępnianie informacji

[1] Rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 910/2014 z dnia 23 lipca 2014 r. w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym oraz uchylające dyrektywę 1999/93/WE (Dz. U. UE. L. z 2014 r. Nr 257, str. 73), dalej zwane rozporządzeniem eIDAS.

o dostawcach usług zaufania). Wśród podanych tam celów nie ma informacji o kwalifikowanych usługach zaufania jakie dostawcy ci świadczą. Organ ds. ochrony danych osobowych sugeruje rozważenie rozszerzenia zakresu celów.

W **art. 23 projektu** upoważnia się Radę Ministrów do wydania rozporządzenia w zakresie wymagań organizacyjno-technicznych krajowej infrastruktury zaufania. Po pierwsze należy wskazać, iż użycie określenia „w szczególności" nie powinno być dopuszczone jako nieprawidłowa delegacja do wydania aktu wykonawczego, która powinna być precyzyjna i wyczerpująca. Po drugie, w sytuacji przetwarzania danych osobowych w ramach krajowej infrastruktury nie powinno się wskazywać ich zakresu w akcie podustawowym. Zgodnie z **art. 51 ust. 3 Konstytucji RP** ujawnianie informacji dotyczących osoby może mieć miejsce tylko na podstawie ustawy. Generalny Inspektor sugeruje wskazanie zakresu danych osobowych w ramach przygotowywanego projektu. Organ ds. ochrony danych osobowych jest także bezpośrednio zainteresowany odpowiednim określeniem zasad zawiadamiania przez dostawców usług zaufania organów nadzoru oraz właściwych organów (w tym organu ochrony danych) i zasad ich wzajemnej współpracy w przypadku stwierdzenia nieprawidłowości w świadczeniu usług zaufania, w szczególności w zakresie prawidłowego przetwarzania danych osobowych przez wszystkie zaangażowane podmioty. Będzie to oczywiście przedmiotem dalszych prac legislacyjnych, jednak już na obecnym etapie należy tę kwestię podnieść.

W **art. 24 projektu** wskazano, że organ nadzoru może upoważnić Narodowy Bank Polski, na wniosek jego Prezesa, do wykonywania części zadań organu nadzoru. Kwestia ta nie została wyjaśniona w uzasadnieniu do projektu. Generalny Inspektor uprzejmie prosi o wyjaśnienie tej propozycji oraz jej wpływu na wykonywanie przez w/w podmioty zadań nadzorczych (w tym przetwarzanie danych osobowych), w szczególności informowania organu ochrony danych o naruszeniach mających wpływ na ochronę danych osobowych. Rozporządzenie eIDAS przewiduje taką możliwość w art. 17 ust. 4 lit. h, jednakże przede wszystkim w zakresie prowadzenia krajowej listy zaufania.

W **art. 28 ust. 1 pkt 1 projektu** zaproponowano odwołanie do rozporządzenia wydanego na podstawie ust. 5, który dotyczy kar pieniężnych. Prawidłowym byłoby odwołanie do ust. 6, który stanowi delegację ustawową do wydania rozporządzenia, o którym mowa w ust. 1.

W **art. 35 ust. 2 projektu** wskazano 20-letni okres retencji dokumentów i danych. Generalny Inspektor prosi o wskazanie uzasadnienia dla tak długiego okresu przechowywania tych informacji. W szczególności koniecznym jest potwierdzenie, czy informacje te będą obejmować dane osobowe przetwarzane w związku ze wszelkimi aspektami świadczenia usług zaufania.

W **art. 38 ust. 1 i 2 projektu** proponuje się wprowadzenie obowiązku przekazania dokumentów i danych związanych ze świadczonymi przez dostawcę usługami do organu nadzoru w przypadku, gdy kwalifikowany dostawca usług zaufania utracił status kwalifikowanego dostawcy. W przepisie tym nie ma jednak wymagań dotyczących zabezpieczenia integralności przekazanych danych w przypadku, jeśli dokumenty lub dane przekazywane są w postaci elektronicznej. Brak ww. wymagań może skutkować tym, że podmiot, który je przekazał może wyprzeć się ich treści uzasadniając to tym, że organ nadzoru dokonał ich zmiany. W związku z powyższym należy rozważyć dodanie w przedmiotowych przepisach warunku zapewniającego integralność przekazanych danych poprzez wykonanie dla nich np. odpowiedniej funkcji skrótu.

Zmiany wprowadzane **art. 54 projektu** do ustawy z dnia 14 czerwca 1960 r. Kodeks Postępowania Administracyjnego (t.j. Dz. U. z 2016 r. poz. 23) nie przewidują wykorzystania środka identyfikacji, jakim jest pieczęć elektroniczna przewidziana w rozporządzeniu eIDAS, co pozwalałoby wyeliminować zgłaszane przez organ ds. ochrony danych osobowych nieprawidłowości ujawniania takich danych jak numer PESEL urzędników, którzy zobowiązani są podpisywać pisma urzędowe swoim podpisem kwalifikowanym działając w imieniu instytucji, w której są zatrudnieni. Kwestia ta była sygnalizowana wielokrotnie Ministrowi Gospodarki przez Generalnego Inspektora w toku wcześniejszych prac nad projektem rozporządzenia (sygn. pism DOLiS-072-24/12/74040, DOLiS-072-24/13/56012, DOLiS-072-24/13/70303, DOLiS-072-24/13/74360). Generalny Inspektor stoi na stanowisku, iż numer PESEL nie powinien być elementem udostępnianym przy podpisach elektronicznych, jako że stanowi podstawę systemu ewidencji ludności oraz jest daną nie powiązaną z działaniami o charakterze służbowym. Atrybut ten mógłby być wykorzystywany, przekazywany jedynie w celu weryfikacji oraz tylko gdy wymagają tego przepisy prawa i o ile takie obowiązki projektodawca chciałby nałożyć na usługobiorców. Nowe podpisy elektroniczne wydawane użytkownikom powinny takie rozwiązanie przewidywać.

W **kolejnych przepisach zmieniających** stosuje się rozróżnienie określając w jednych przypadkach konieczność:

1. opatrzenia kwalifikowanym podpisem elektronicznym, a w innych
2. opatrzenia kwalifikowanym podpisem elektronicznym w rozumieniu przepisów o usługach zaufania.

Wątpliwość Generalnego Inspektora budzi kwestia, czy rozróżnienie to wynika z przyjęcia szczególnych definicji podpisu elektronicznego w tych ustawach, czy też projektodawca realizuje w ten sposób inny cel.

Z uwagi na doniosłość projektu dla rozwoju rynku cyfrowego w Polsce oraz konieczność ochrony danych jego uczestników Generalny Inspektor Ochrony Danych Osobowych deklaruje swój aktywny udział w pracach nad projektem oraz zastrzega możliwość zgłaszania dalszych uwag na etapie rządowym i w toku prac sejmowych.