PREZES
URZĘDU OCHRONY
DANYCH OSOBOWYCH
Mirosław Wróblewski

Warszawa, dnia 12-09-2024

DOL.413.3.2024

Pan
Krzysztof Gawkowski
Wiceprezes Rady Ministrów
Minister Cyfryzacji

ePUAP: /MAiC/SkrytkaESP

Szanowny Panie Premierze,

działając na podstawie art. 52 ust. 2 ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych[1] zwracam się **z uprzejmą prośbą i wnioskiem o podjęcie prac legislacyjnych prowadzących do zmiany przepisów ustawy o usługach zaufania oraz identyfikacji elektronicznej[2] poprzez przyjęcie rozwiązań, które eliminowałyby ujawnianie numeru PESEL w certyfikacie kwalifikowanego podpisu elektronicznego celem dostosowania aktualnych regulacji prawnych dotyczących kwalifikowanego podpisu elektronicznego do zasad wyrażonych w przepisach rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679[3]**.

Impulsem do niniejszego wystąpienia są sygnały napływające do organu nadzorczego do spraw ochrony danych osobowych od podmiotów danych posługujących się kwalifikowanymi podpisami elektronicznymi, jak i reprezentujących je organizacji, wskazujące na obawy utraty kontroli nad danymi osobowymi w szczególności w postaci numeru PESEL. Sygnalizowane organowi wątpliwości wynikają z tego, że numer PESEL jest pozyskiwany przez dostawców usług zaufania publicznego (kwalifikowanego podpisu

[1] Dz. U. z 2019 r. poz. 1781.
[2] Ustawa z dnia 5 września 2016 r. o usługach zaufania oraz identyfikacji elektronicznej (Dz. U. z 2024 r. poz. 422).
[3] Rozporządzenie 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. Urz. UE L 119 z 4.5.2016, str. 1 ze zm.).

elektronicznego), a następnie jest upubliczniany, co z kolei nie wynika ani z przepisów europejskich, ani krajowych.

Stosowanie certyfikatu kwalifikowanego podpisu elektronicznego regulują przepisy rozporządzenia 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 uchylającego dyrektywę 1999/93/WE [4] (dalej jako: „rozporządzenie eIDAS"), oraz ustawy z dnia 5 września 2016 r. o usługach zaufania oraz identyfikacji elektronicznej (dalej jako: „ustawa o usługach zaufania").

Art. 26 rozporządzenia eIDAS określa wymaganie, że zaawansowany podpis elektroniczny musi być unikalnie przyporządkowany podpisującemu, umożliwiać ustalenie tożsamości podpisującego przy użyciu danych służących do składania podpisu elektronicznego, których podpisujący może, z dużą dozą pewności, użyć pod wyłączną swoją kontrolą oraz być powiązany z danymi podpisanymi w taki sposób, że każda późniejsza zmiana danych jest rozpoznawalna. Identyfikacja elektroniczna oznacza proces używania danych w postaci elektronicznej identyfikujących osobę, unikalnie reprezentujących osobę fizyczną lub prawną. Dane identyfikujące osobę oznaczają zestaw danych, który jest wydawany zgodnie z prawem Unii lub prawem krajowym i który umożliwia ustalenie tożsamości osoby fizycznej lub prawnej, lub osoby fizycznej reprezentującej inną osobę fizyczną lub osobę prawną, a dane służące do składania podpisu elektronicznego oznaczają unikalne dane, których podpisujący używa do składania podpisu elektronicznego (art. 3 rozporządzenia eIDAS). Powyższe odnosi się do zestawienia danych jednoznacznie identyfikujących podmiot w obrocie prawnym.

Rozporządzenie eIDAS w art. 3 pkt 14 definiuje certyfikat podpisu elektronicznego jako poświadczenie elektroniczne, które przyporządkowuje dane służące do walidacji podpisu elektronicznego do osoby fizycznej i potwierdza co najmniej imię i nazwisko lub pseudonim tej osoby. Natomiast kwalifikowany certyfikat podpisu elektronicznego oznacza certyfikat podpisu elektronicznego, który jest wydawany przez kwalifikowanego dostawcę usług zaufania i spełnia wymogi określone w załączniku I (art. 3 pkt 15 rozporządzenia eIDAS). W ww. załączniku nr I wskazano, że kwalifikowany certyfikat zawiera co najmniej imię i nazwisko podpisującego lub jego pseudonim; jeżeli używany jest pseudonim, fakt ten jest jasno wskazany oraz zawiera kod identyfikacyjny certyfikatu, który musi być niepowtarzalny dla kwalifikowanego dostawcy usług zaufania.

W świetle powyższych regulacji, o ile zrozumiałe jest, że kod identyfikacyjny certyfikatu powinien opierać się na numerze z rejestru publicznego, który jednoznacznie identyfikowałby osobę posługującą się kwalifikowanym podpisem elektronicznym, to używanie do tego celu numeru PESEL budzi liczne kontrowersje, ponieważ **rozwiązania przyjęte przez unijnego ustawodawcę nie wskazują oczywiście na obligatoryjne używanie numeru PESEL w treści certyfikatu kwalifikowanego podpisu elektronicznego.**

Zgodnie z art. 14 ustawy o usługach zaufania kwalifikowany dostawca usług zaufania, wydając kwalifikowany certyfikat podpisu elektronicznego, jest obowiązany uzyskać od osoby ubiegającej się o certyfikat potwierdzenie przyporządkowania do niej

[4] Dz. Urz. UE L 257 z 28.08.2014 ze zm.

danych służących do weryfikacji podpisu elektronicznego, które są zawarte w wydanym certyfikacie oraz poinformować osobę ubiegającą się o certyfikat o procedurze zgłaszania żądań unieważnienia kwalifikowanego certyfikatu. Artykuł 21q tej ustawy stanowi natomiast, że podmiot odpowiedzialny za system identyfikacji elektronicznej przetwarza dane osobowe osób, którym w tym systemie wydano środki identyfikacji elektronicznej, obejmujące: imię (imiona), nazwisko, nazwisko rodowe, numer PESEL lub niepowtarzalny identyfikator środka identyfikacji elektronicznej, o którym mowa w przepisach wydanych na podstawie art. 12 ust. 8 rozporządzenia 910/2014, datę urodzenia, miejsce urodzenia, płeć, adres zamieszkania. Powyższe nie oznacza jednak, że wszystkie ww. dane służące tworzeniu środka identyfikacji elektronicznej powinny być również upubliczniane. Dodać należy, że nowelizacja rozporządzenia eIDAS, która obowiązuje od 20 maja br. w odniesieniu do ram interoperacyjności wprowadziła nowe kryterium dotyczące wdrożenia zasad prywatności i bezpieczeństwa na etapie projektowania (art. 12 ust. 3 lit. c) oraz wskazała, że zawierają one odniesienie do minimalnego zbioru danych identyfikujących osobę niezbędnych do niepowtarzalnego reprezentowania osoby fizycznej lub prawnej, lub osoby fizycznej reprezentującej inną osobę fizyczną lub osobę prawną, które jest dostępne w ramach systemów identyfikacji elektronicznej (art. 12 ust. 4 lit d).

Organ nadzorczy wielokrotnie w swoich stanowiskach zwracał uwagę, że numer PESEL jest daną wyjątkową, ponieważ identyfikuje w sposób unikalny daną osobę i pozwala na ustalenie szeregu dodatkowych informacji takich jak płeć, czy wiek tej osoby. W rozumieniu art. 87 RODO[5] jest on krajowym numerem identyfikacyjnym, którego przetwarzanie powinno odbywać się z zachowaniem odpowiednich zabezpieczeń praw i wolności osoby, której dane dotyczą, przewidzianych w ogólnym rozporządzeniu o ochronie danych. W świetle krajowych przepisów stanowiących o numerze PESEL (art. 3 ustawy o ewidencji ludności[6]) ma on służyć do ewidencjonowania ludności, jednakże podpis kwalifikowany, który zawiera w swojej treści również tę daną osobową wykorzystywany jest w celu identyfikacji nie tylko do celów prywatnych osoby, ale także w ramach jej działalności zawodowej.

Możliwość powiązania informacji z wielu powszechnie dostępnych baz danych/rejestrów, których łącznikiem jest numer PESEL uznawany za tzw. daną referencyjną, stwarza **ryzyko tworzenia profili osobowych, co jeśli odbywa się bez wiedzy osoby, może stanowić zagrożenie dla jej prywatności, w tym prawa do ochrony danych osobowych**.

Zauważyć należy, że w celu zwiększenia ochrony przed nadużyciami wynikającymi z kradzieży danych ustawodawca[7] wprowadził rozwiązanie umożliwiając osobie, której dane dotyczą, **nieodpłatne zastrzeżenie oraz cofnięcie zastrzeżenia jej**

[5] Zgodnie z art. 87 RODO: Państwa członkowskie mogą określić szczególne warunki przetwarzania krajowego numeru identyfikacyjnego lub innego identyfikatora o zasięgu ogólnym. W takim przypadku krajowego numeru identyfikacyjnego lub innego identyfikatora o zasięgu ogólnym używa się wyłącznie z zachowaniem odpowiednich zabezpieczeń praw i wolności osoby, której dane dotyczą, które przewiduje niniejsze rozporządzenie.

[6] Ustawa z dnia 24 września 2010 r. o ewidencji ludności (Dz. U. z 2024 r. poz. 736).

[7] Mocą ustawy z dnia 7 lipca 2023 r. o zmianie niektórych ustaw w celu ograniczania niektórych skutków kradzieży tożsamości (Dz. U. poz. 1394).

numeru PESEL. W świetle powyższego pojawia się zasadnicze pytanie o możliwość realizacji celów ww. regulacji w sytuacji upubliczniania numeru PESEL w podpisywanych dokumentach.

Przypomnienia wymaga, że organ nadzorczy wielokrotnie zwracał się do resortu cyfryzacji[8], w związku z opiniowaniem aktów prawnych dotyczących przedmiotowego zagadnienia, o podjęcie pogłębionej debaty dotyczącej zasad wykorzystywania numeru PESEL w obowiązującym porządku prawnym. Wskazywał w nich, że dostępne są inne identyfikatory niż numer PESEL, jak np. numer paszportu, numer dowodu osobistego lub numer identyfikacji podatkowej, które mogłyby być stosowane do uwierzytelniania osoby podpisującej dokument, a jednocześnie w mniejszym stopniu ingerowałyby w jej gwarantowane Konstytucją RP prawo ochrony danych osobowych. Posługiwanie się cechami z tych dokumentów w ocenie organu nadzorczego wydaje się być mniej ryzykowne dla podmiotów danych niż posługiwanie się numerem PESEL, ponieważ dokumenty te łatwiej wycofać z obrotu i ich cechy są w nim obecne jedynie przez określony czas.

Możliwość pozyskania określonych danych osobowych we wniosku o wystawienie takiego certyfikatu podpisu nie powinna oznaczać, że dane te powinny być zamieszczone w treści podpisu kwalifikowanego oraz publikowane po elektronicznym podpisaniu dokumentu. Przepisy prawa nie przewidują bowiem obowiązku ujawniania numeru PESEL w dokumencie opatrzonym podpisem elektronicznym. Również ogólne rozporządzenie o ochronie danych w art. 6 ust. 1 lit. c odnosząc się do jednej z podstaw legalizujących przetwarzanie danych stanowi, że przetwarzanie jest zgodne z prawem jedynie w sytuacji, jeżeli jest niezbędne do wypełnienia obowiązku prawnego ciążącego na administratorze. **O ile więc zasadnym jest użycie numeru PESEL w przypadku weryfikacji osoby wnioskującej o wydanie certyfikatu kwalifikowanego podpisu elektronicznego, to zdecydowanie wątpliwe jest ujawnianie tej informacji innym osobom uzyskującym dostęp do treści podpisu.**

W czerwcu 2019 r. organ nadzorczy skierował wystąpienie do Ministerstwa Cyfryzacji[9], którego tematyka była poruszana na spotkaniach organizowanych przez Ministra Cyfryzacji z udziałem przedstawicieli organu ochrony danych w związku z dyskusją odnoszącą się do ograniczania ryzyk związanych z kradzieżą tożsamości. Niemniej postulaty organu nadzorczego do tej pory nie przyniosły oczekiwanych rezultatów, a sygnalizowany wówczas problem narasta.

Ujawnianie numeru PESEL także w certyfikacie podpisu zaufanego jest problemem poruszanym przez szereg środowisk i organów (m.in. dostrzegł go Rzecznik Praw Obywatelskich, związki zawodowe, organizacje pozarządowe). Dlatego też organ nadzorczy pragnie wskazać na konieczność podjęcia prac legislacyjnych prowadzących do zmian przepisów, które powinny doprowadzić do ograniczenia wykorzystywania numeru PESEL w certyfikatach podpisów elektronicznych, których użycie prowadzi do ujawniania numeru PESEL.

---

[8] Pisma: z 2 listopada 2020 r. sygn. DOL.401.477.2020, z 19 marca 2021 r. sygn. DOL.401.102.2021, z 7 czerwca 2021 r. sygn. DOL.401.241.2021, z 22 czerwca 2022 r. sygn. DOL.401.276.2022.

[9] Pismo z 14 czerwca 2019 r. sygn. ZSPU.023.97.2019.PM.

Powyższe kwestie powinny być również poddane analizie pod kątem wyrażonych w Konstytucji RP: zasady legalizmu[10], zasady wolności[11] oraz prawa ochrony danych osobowych[12].

W razie pozytywnej decyzji Pana Premiera i podjęcia prac przez resort cyfryzacji w związku z przedstawionym powyżej zagadnieniem **Prezes Urzędu Ochrony Danych deklaruje wsparcie eksperckie przy wypracowywaniu nowych rozwiązań prawnych.**

Łączę wyrazy szacunku

Mirosław Wróblewski
Prezes Urzędu
Ochrony Danych Osobowych

/dokument w postaci elektronicznej
podpisany kwalifikowanym podpisem elektronicznym/

[10] Zgodnie z art. 7 Konstytucji RP: Organy władzy publicznej działają na podstawie i w granicach prawa.
[11] Zgodnie z art. 31 Konstytucji RP: 1. Wolność człowieka podlega ochronie prawnej. 2. Każdy jest obowiązany szanować wolności i prawa innych. Nikogo nie wolno zmuszać do czynienia tego, czego prawo mu nie nakazuje. 3. Ograniczenia w zakresie korzystania z konstytucyjnych wolności i praw mogą być ustanawiane tylko w ustawie i tylko wtedy, gdy są konieczne w demokratycznym państwie dla jego bezpieczeństwa lub porządku publicznego, bądź dla ochrony środowiska, zdrowia i moralności publicznej, albo wolności i praw innych osób. Ograniczenia te nie mogą naruszać istoty wolności i praw.
[12] Zgodnie z art. 51 Konstytucji RP: 1. Nikt nie może być obowiązany inaczej niż na podstawie ustawy do ujawniania informacji dotyczących jego osoby. 2. Władze publiczne nie mogą pozyskiwać, gromadzić i udostępniać innych informacji o obywatelach niż niezbędne w demokratycznym państwie prawnym. 3. Każdy ma prawo dostępu do dotyczących go urzędowych dokumentów i zbiorów danych. Ograniczenie tego prawa może określić ustawa. 4. Każdy ma prawo do żądania sprostowania oraz usunięcia informacji nieprawdziwych, niepełnych lub zebranych w sposób sprzeczny z ustawą. 5. Zasady i tryb gromadzenia oraz udostępniania informacji określa ustawa.