Biometryczna weryfikacja tożsamości klientów usług płatniczych

Posted on 2024-04-30

Przetwarzanie przez instytucje finansowe danych biometrycznych klientów na potrzeby weryfikacji ich tożsamości nie powinno być podstawową, a tym bardziej jedyną stosowaną w tym celu metodą. Natomiast wyłączną przesłanką legalizującą takie działanie powinna być wyraźna i świadoma zgoda osób, których dane dotyczą.

W związku z trwającą w środowisku finansistów dyskusją i wpływającymi pytaniami, UODO zajmował się w ostatnim czasie kwestią wykorzystywania analiz behawioralnych w celu ograniczania transakcji oszukańczych w płatnościach bezgotówkowych.

Ponieważ korzystanie z tej technologii stanowi głęboką ingerencję w – zagwarantowane przepisami Karty Praw Podstawowych Unii Europejskiej (art. 7 i art. 8 ust. 1), Konstytucji RP (art. 47 i art. 51) oraz RODO – prawo do prywatności i prawo do ochrony danych osobowych, zagadnienie to budzi szczególne zainteresowanie organu nadzorczego w kontekście zgodności z zasadami ochrony danych osobowych.

Szczególne dane wymagają wzmożonej ochrony

Stosowanie przez instytucje finansowe analizy behawioralnej (np. sposobu pisania na klawiaturze czy sposobu poruszania myszą komputera) i tworzenie na podstawie cech charakterystycznych dla danego użytkownika jego unikalnego profilu oraz późniejsze wykorzystywanie tych danych w celu uwierzytelniania klientów usług płatniczych wiąże się z przetwarzaniem danych biometrycznych
w rozumieniu art. 4 pkt 14 RODO, które należą do danych szczególnych kategorii i których wykorzystywanie – stosownie do art. 9 RODO – podlega wzmocnionej ochronie.

Dane biometryczne w RODO i Wytycznych

Stosownie do art. 4 pkt 14 RODO „dane biometryczne" oznaczają dane, które wynikają ze specjalnego przetwarzania technicznego, dotyczą cech fizycznych, fizjologicznych lub specjalnego przetwarzania technicznego oraz umożliwiają lub potwierdzają jednoznaczną identyfikację tej osoby, takie jak wizerunek twarzy lub dane daktyloskopijne.

Dane biometryczne są danymi szczególnej kategorii w rozumieniu art. 9 ust. 1 RODO.

Wiele cennych informacji i wskazówek dotyczących danych biometrycznych i ich przetwarzania zawartych jest w takich dokumentach, jak przyjęta 27 kwietnia 2012 r. Opinia 3/2012 Grupy Roboczej Art. 29 w sprawie zmian sytuacji w dziedzinie technologii biometrycznych (WP 193) czy przyjęte 29 stycznia 2020 r. Wytyczne 3/2019 w sprawie przetwarzania danych osobowych przez urządzenia wideo.

Europejska Rada Ochrony Danych (EROD) w Wytycznych 3/2019 wskazała, że aby dane były uznane za biometryczne należy wziąć pod uwagę łącznie trzy elementy: 1) charakter danych – dane dotyczą cech fizycznych, fizjologicznych lub behawioralnych danej osoby fizycznej, 2) środki i sposób przetwarzania wynikać muszą z użycia odpowiedniej technologii oraz 3) dane są przetwarzane
w celu jednoznacznej identyfikacji osoby fizycznej.

Jednocześnie w dobie szybkiego rozwoju nowoczesnych technologii przetwarzania danych,

zwłaszcza takich jak te oparte na algorytmach sztucznej inteligencji, można zakładać, że unikalne profile klientów dostawców usług płatniczych pozwolą na uzyskanie dodatkowych jeszcze informacji, których ostateczny zakres trudno obecnie przewidzieć.

Dlatego każda decyzja administratora o pozyskiwaniu danych opartych na biometrii powinna być poprzedzona szczególnie wnikliwą analizą. Przetwarzanie takich danych powinno się odbywać nie tylko z poszanowaniem zasady legalności (art. 5 ust. 1 lit. a RODO), ale także być działaniem adekwatnym oraz stosownym i ograniczonym z punktu widzenia realizacji zakładanego celu (art. 5 ust. 1 lit. c RODO).

Takie stanowisko znajduje potwierdzenie w orzecznictwie Trybunału Konstytucyjnego, m.in. w wyroku z 11 kwietnia 2000 r. (sygn. akt K 15/98), w którym TK stwierdza, że: „poszukując odpowiedzi na pytanie, czy ingerencja w sferę konstytucyjnego prawa jednostki jest zgodna z zasadą konieczności, należy rozważyć, czy cel, do którego dąży ustawodawca można osiągnąć przy pomocy środków równie skutecznych, ale mniej uciążliwych dla jednostki”.

W świetle powyższego przed wprowadzeniem do stosowania tego rodzaju technik identyfikacji klientów instytucje finansowe powinny przedstawić szczegółowe analizy co do tego, czy rzeczywiście zasadne jest przyjęcie, że podstawowa metoda weryfikacji klienta musi być oparta na analizie jego cech biometrycznych. Instrumentami pomocnymi w dokonaniu takiej oceny są zarówno analiza ryzyka, jak i ocena skutków dla ochrony danych (art. 35 RODO).

Jednocześnie podkreślić należy, że w świetle RODO zasadą jest zakaz przetwarzania danych biometrycznych (art. 9 ust. 1 RODO), a odstępstwo od niego powinno mieć wyraźne oparcie w jednym z wyjątków wprost wymienionych w ust. 2 tego przepisu.

Przepisy sektorowe nie dają odpowiednich gwarancji
Dokonując analizy dopuszczalności przetwarzania danych biometrycznych w celu uwierzytelniania klientów usług płatniczych w pierwszej kolejności rozważyć należy, czy

obowiązujące przepisy prawa krajowego regulujące działalność instytucji finansowych pozwalają na przetwarzanie danych biometrycznych do takich celów.

Artykuł 9 ust. 2 lit. g RODO przewiduje, że dane szczególnych kategorii mogą być przetwarzane, gdy jest to niezbędne ze względów związanych z ważnym interesem publicznym, na podstawie prawa Unii lub prawa państwa członkowskiego, które są proporcjonalne do wyznaczonego celu, nie naruszają istoty prawa do ochrony danych i przewidują odpowiednie i konkretne środki ochrony praw podstawowych i interesów osoby, której dane dotyczą.

Wskazać należy, że istniejące przepisy prawa nie mogą stanowić podstawy prawnej do stosowania przez dostawców usług płatniczych systemów gromadzących dane biometryczne. Art. 10 ustawy z 19 sierpnia 2011 r. o usługach płatniczych stanowiący, że dostawcy, organizacje płatnicze i podmioty prowadzące systemy płatności przetwarzają dane osobowe w zakresie niezbędnym do zapobiegania oszustwom związanym z wykonywanymi usługami płatniczymi, prowadzeniem schematu płatniczego lub prowadzeniem systemu płatności oraz dochodzenia i wykrywania tego rodzaju oszustw przez właściwe organy, nie uprawnia banków i innych instytucji sektora finansowego do przetwarzania danych biometrycznych w celu dotyczącym zapobiegania oszustwom. Przepis ten nie przewiduje bowiem odpowiednich gwarancji dla ochrony praw i interesów osób, których dane miałyby być przetwarzane. W szczególności nie przewiduje, jakie dane i w jakim zakresie miałyby być przetwarzane w tym celu, czy w każdej sytuacji, czy jedynie w przypadkach konkretnych wątpliwości co do tożsamości osoby dokonującej płatności, i w jaki konkretnie sposób. Dodatkowo wskazać należy, że obecne brzmienie art. 10 ustawy o usługach płatniczych zostało nadane art. 118 ustawy z dnia 21 lutego 2019 r. o zmianie niektórych ustaw w związku z zapewnieniem stosowania 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). W wersji ustawy sprzed 4 maja 2019 r. przepis ten stanowił wprost o danych osobowych szczególnych kategorii jako wyłączonych z przetwarzania, stanowiąc o przetwarzaniu „(…) z wyjątkiem danych, o których mowa w art. 9 ust. 1 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 […]". Treść zmienionego art. 10 nie została jednak wzbogacona o jakiekolwiek elementy gwarancyjne dla podmiotów danych, a zatem nie może być uznana za odpowiednią podstawę przetwarzania danych biometrycznych przez instytucję finansową.

Zgoda i warunki jej wyrażania

W tej sytuacji w ocenie organu nadzorczego jedyną przesłanką, która mogłaby być brana pod uwagę jako podstawa legalizacji przetwarzania danych biometrycznych przez instytucje finansowe, jest świadoma i wyraźna zgoda osoby, której dane dotyczą, a zatem przesłanka wskazana w art. 9 ust. 2 lit. a RODO. Żeby można było mówić o wyrażeniu zgody wyraźnej, konieczne jest, by administrator poinformował ją o ryzykach związanych z przetwarzaniem takich danych, zasadach ich przetwarzania, stosowanych zabezpieczeniach i przysługujących jej uprawnieniach. Zgoda powinna także wyraźnie precyzować cel przetwarzania w momencie jej odbierania. Powinna istnieć również alternatywna metoda, z której podmiot danych mógłby skorzystać w przypadku braku zgody tak, aby nie zostać pozbawionym możliwości skorzystania z konkretnej usługi.

Analizie poddane powinno być także stanowisko EROD wyrażone w Wytycznych 6/2020 w sprawie wzajemnych zależności między dyrektywą PSD2 a RODO". EROD wskazuje m.in., że: „Prawnie uzasadnionym interesem dostawcy usług płatniczych, którego sprawa dotyczy, może być przetwarzanie danych osobowych bezwzględnie niezbędne do zapobiegania oszustwom, o ile charakteru nadrzędnego nie mają interesy lub podstawowe prawa i wolności osoby, której dane dotyczą. Czynności przetwarzania w celu zapobiegania nadużyciom powinny opierać się na starannej ocenie poszczególnych przypadków przez administratora zgodnie z zasadą rozliczalności". W ww. Wytycznych EROD wskazuje, że:

„Wyraźna zgoda, o której mowa w art. 94 ust. 2 PSD2, jest zgodą umowną. Oznacza to, że art. 94 ust. 2 PSD2 należy interpretować w ten sposób, że zawierając umowę z dostawcą usług płatniczych na podstawie tej dyrektywy, osoby, których dane dotyczą, muszą być w pełni świadome szczególnych kategorii danych osobowych, które będą przetwarzane.

Ponadto należy poinformować je o konkretnym celu (usługa płatnicza), w którym ich dane osobowe będą przetwarzane, i muszą one wyraźnie zgodzić się na te klauzule. Klauzule takie powinny wyraźnie odróżniać się od pozostałych kwestii poruszanych w umowie, a osoba, której dane dotyczą, musiałaby wyraźnie je zaakceptować".

Wskazać należy, że zgodnie z art. 7 ust. 3 RODO osoba, której dane dotyczą, może w dowolnym momencie wycofać zgodę. Wycofanie zgody musi być równie łatwe jak jej wyrażenie. Zgodnie z motywem 59 RODO administrator powinien przewidzieć procedury ułatwiające osobie, której dane dotyczą, wykonywanie praw przysługujących jej zgodnie z RODO, w tym mechanizmy żądania – i gdy ma to zastosowanie bezpłatnego uzyskiwania – w szczególności dostępu do danych osobowych i ich sprostowania lub usunięcia oraz możliwości wykonywania prawa do sprzeciwu. Odmowa udzielenia zgody nie powinna wpływać niekorzystnie na sytuację klienta.

W kontekście zgody, która powinna być odbierana przez bank od klienta, należy także zwrócić uwagę na regulację art. 22 RODO dotyczącą profilowania. Weryfikacja za pomocą urządzeń opartych na technikach analizy behawioralnej powinna być przeanalizowana pod kątem zgodności z postanowieniami ww. przepisu, który w ust. 1 przewiduje że: „Osoba, której dane dotyczą, ma prawo do tego, by nie podlegać decyzji, która opiera się wyłącznie na zautomatyzowanym przetwarzaniu, w tym profilowaniu, i wywołuje wobec tej osoby skutki prawne lub w podobny sposób istotnie na nią wpływa". Wyjątki dopuszczające stosowanie przez administratora tego rodzaju metod przewiduje ust. 2 tego przepisu. W kontekście analizowanych przepisów, przyjmując, że weryfikacja klienta przy pomocy jego danych behawioralnych będzie zachodzić wyłącznie po spełnieniu warunków określonych w

art. 22 ust. 2 lit. c RODO, zgoda wyraźna powinna być rozumiana w sposób analogiczny do tej, o której stanowi art. 9 ust. 2 lit. a RODO. Istotne jest także, aby bank, stosując metody oparte na profilowaniu, uwzględnił w procesie przetwarzania wymagania stawiane przez art. 22 ust. 3 RODO, który nakłada na administratora obowiązek wprowadzenia gwarancji dotyczących możliwości zakwestionowania decyzji: „W przypadkach, o których mowa w ust. 2 lit. a) i c), administrator wdraża właściwe środki ochrony praw, wolności i prawnie uzasadnionych interesów osoby, której dane dotyczą, a co najmniej prawa do uzyskania interwencji ludzkiej ze strony administratora, do wyrażenia własnego stanowiska i do zakwestionowania tej decyzji".

Konkluzja

Przy wszystkich wskazanych wyżej uwagach i zastrzeżeniach przyjąć należy, że przetwarzanie przez instytucje finansowe danych biometrycznych klientów nie powinno być podstawową metodą weryfikacji tożsamości klienta. Zbieranie takich danych na podstawie zgody klienta obwarowane zaś jest szeregiem szczegółowych warunków, których spełnienie jest decydujące dla legalności tego procesu.