Daniel Trędkiewicz
Aplikant radcowski w Kancelarii FORYSTEK & PARTNERZY Adwokaci i Radcowie Prawni, Inspektor Ochrony Danych w podmiotach świadczących usługi drogą elektroniczną, członek Stowarzyszenia Praktyków Ochrony Danych.

Weryfikacja tożsamości na podstawie skanu dowodu osobistego przez podmioty świadczące usługi drogą elektroniczną

Weryfikacja tożsamości na podstawie skanu dowodu osobistego jest jednym z najczęściej kwestionowanych sposobów autoryzacji użytkowników w Internecie. Taką metodę często stosują podmioty świadczące usługi drogą elektroniczną, które nie mają możliwości przeprowadzenia weryfikacji na podstawie bezpośredniego kontaktu fizycznego z użytkownikiem. Analiza przepisów i orzecznictwa prowadzi do wniosku, że przy spełnieniu odpowiednich warunków, taki sposób potwierdzania tożsamości usługobiorców będzie dopuszczalny.

Po rozpoczęciu obowiązywania RODO przedsiębiorcy napotkali szereg problemów związanych z obsługą żądań z zakresu ochrony danych osobowych. Wśród podmiotów świadczących usługi drogą elektroniczną jednym z największych wyzwań w tym zakresie jest konieczność potwierdzenia tożsamości osoby chcącej skorzystać ze swoich uprawnień. Realizacja dyspozycji złożonej przez nieumocowaną do tego osobę może stanowić naruszenie ochrony danych osobowych, dlatego administrator powinien wprowadzić skuteczne procedury zapobiegające wykonywaniu żądań składanych przez osoby nieuprawnione. Obowiązkiem administratora jest stosowanie odpowiednich środków technicznych i organizacyjnych mających na celu ochronę praw osób, których dane dotyczą, dlatego to administrator na podstawie znajomości własnej organizacji powinien ustalić jakie metody weryfikacji tożsamości będą w jego przypadku adekwatne i przyniosą oczekiwane skutki.

Metodą, która zwykle wywołuje najwięcej kontrowersji jest weryfikacja tożsamości osoby składającej wniosek na podstawie skanu dowodu osobistego. W trosce o swoją prywatność oraz w obawie o nieuprawnione wykorzystanie skanu dokumentu, osoby wnoszące żądanie z zakresu ochrony danych osobowych często sprzeciwiają się takiej weryfikacji, uznając ją za działanie bezprawne. Również polski organ nadzorczy podczas wymiany uwag z Prezesem Związku Banków Polskich w sprawie dopuszczalności kserowania dowodów osobistych przez banki w pewnym sensie podważył legalność takiego działania, wskazując że „sporządzenie kopii dowodów tożsamości w ocenie organu nadzorczego jest legalne je-

dynie wtedy, kiedy wynika to wprost z przepisów rangi ustawy"[1]. Nie przedstawiono jednak szerszej argumentacji skąd taki warunek miałby wynikać, a stanowisko organu nadzorczego słusznie zostało poddane krytyce. Brak jest bowiem powszechnie obowiązującego przepisu, który potwierdzałby zasadność poglądu Prezesa Urzędu Ochrony Danych Osobowych. Po rozpoczęciu obowiązywania RODO nic się w tym zakresie nie zmieniło, co znajduje potwierdzenie również w informacjach przekazywanych przez unijne organy. W odpowiedzi Komisji Europejskiej na interpelację europosła Adama Szejnfelda w sprawie kopiowania dokumentów stwierdzających tożsamość przekazano informację, że przepisy RODO nie zakazują takiej czynności[2]. Również w praktyce orzeczniczej przyjęło się, że gromadzenie danych osobowych poprzez wykonanie kopii dokumentu zawierającego te dane jest jedynie czynnością techniczną. Natomiast posługiwanie się taką czy inną techniką utrwalania tych danych (kopiowanie lub przepisywanie) nie przesądza samo przez się o legalności albo nielegalności takiego przetwarzania danych[3]. Co istotne, stanowisko takie również prezentował w okresie obowiązywania ustawy o ochronie danych osobowych z 1997 roku Generalny Inspektor Ochrony Danych Osobowych[4].

Podczas weryfikacji tożsamości na podstawie skanu dowodu osobistego istotne jest jednak postępowanie w sposób zgodny z zasadą minimalizacji danych, której treścią jest obowiązek przetwarzania tylko tych danych osobowych, które są adekwatne, stosowne oraz ograniczone do tego, co niezbędne do celów, w których są przetwarzane. Aktualnie warstwa graficzna dowodu osobistego zawiera dane dotyczące osoby takie jak (1) nazwisko, (2) imię (imiona), (3) nazwisko rodowe, (4) imiona rodziców, (5) data i miejsce urodzenia, (6) płeć, (7) wizerunek twarzy, (8) numer PESEL oraz (9) obywatelstwo, a także dane dotyczące dowodu osobistego w postaci (1) serii i numeru dowodu osobistego, (2) daty wydania, (3) daty ważności, (4) oznaczenia organu wydającego dowód osobisty oraz (5) numeru CAN. Administrator musi ocenić, które dane z dowodu osobistego są mu niezbędne do prawidłowej weryfikacji tożsamości. Powinien również podjąć odpowiednie środki, by nie przetwarzać danych zbędnych, nadmiarowych. Spośród danych dotyczących dowodu osobistego podczas weryfikacji na odległość zwykle niezbędne okażą się seria i numer dowodu osobistego oraz data jego ważności. Data ważności z uwagi na fakt, że dowód osobisty jest ważny jedynie przez określony czas (odpowiednio 5 lat w przypadku osoby, która nie ukończyła 5 roku życia lub 10 lat w pozostałych przypadkach), natomiast seria i numer dowodu pozwala na dostęp do wykazu zawieszonych i unieważnionych dowodów osobistych na zasadzie art. 74 ustawy o dowodach osobistych[5], co pozwala ograniczyć ryzyko posłużenia się dowodem przez osobę nieuprawnioną. Z danych dotyczących osoby zwykle wystarczające powinny być imię i nazwisko oraz w stosownych przypadkach również numer PESEL. Przy czym pozyskanie numeru PESEL wydaje się uzasadnione głównie wtedy, gdy administrator danych ma możliwość porównania

1 Pismo Prezesa Urzędu Ochrony Danych Osobowych do Prezesa Związku Banków Polskich z sierpnia 2019 r., s. 1;
2 Odpowiedź udzielona przez komisarz Verę Jourovą w imieniu Komisji Europejskiej na pytanie europosła Adama Szejnfelda, numer referencyjny pytania E-001840-18.
3 Wyrok Naczelnego Sądu Administracyjnego z dnia 19 grudnia 2001 r., II SA 2869/00;
4 www.archiwum.giodo.gov.pl/pl/332/2839;
5 Ustawa z dnia 6 sierpnia 2010 roku o dowodach osobistych;

tego numeru z danymi, które już posiada, lub z danymi, które znajdują się w publicznie dostępnych rejestrach do których dostęp ma administrator.

Dopuszczalność jednoczesnego przetwarzania numeru PESEL oraz serii i numeru dowodu osobistego na potrzeby weryfikacji tożsamości potwierdził Prezes Urzędu Ochrony Danych Osobowych w decyzji z dnia 10 grudnia 2018 roku, wskazując że „praktyka żądania dodatkowych danych weryfikacyjnych może wydawać się zbyt restrykcyjna, jednak nie można jej uznać za nadmierną w przedstawionej sytuacji. Żądanie dodatkowych danych identyfikacyjnych ma na celu maksymalną ochronę samych danych znajdujących się w bazie, jak również procedury ich udostępniania. Takie zabezpieczenie ma na celu zapobieżenie udostępnieniu danych osobie nieupoważnionej, przetwarzanych przez B. S.A. informacji stanowiących tajemnicę bankową. Wobec tego, samo udostępnienie danych żądanych na podstawie art. 33 ustawy, powinno nastąpić po uprzedniej, rzetelnej weryfikacji tożsamości osoby wnioskodawcy. Podwójna weryfikacja za pomocą numeru PESEL oraz serii i numeru dowodu osobistego pozwala ustalić w sposób niebudzący wątpliwości tożsamości osoby wnioskodawcy". Wprawdzie decyzja ta dotyczy sektora bankowego, jednakże tożsamą argumentację można zastosować w przypadku administratorów z innych sektorów gospodarki, w tym podmiotów świadczących usługi drogą elektroniczną. Oczywiście to nie oznacza, że łączenie tych danych zawsze będzie uzasadnione, a ostateczny wniosek każdorazowo zależy od konkretnego przypadku.

Podsumowując, nie można wykluczyć dopuszczalności weryfikacji tożsamości przy użyciu skanu dowodu osobistego. Istotne jest jednak właściwe określenie zakresu danych, które pozwolą administratorowi na potwierdzenie, że z wnioskiem wystąpiła osoba uprawniona. Zakres danych musi pozwalać na skuteczną weryfikację, jednakże nie mogą to być dane nadmiarowe, zbierane „na zapas". Z uwagi na zagrożenia dla prywatności przy weryfikacji tożsamości na podstawie skanu dowodu osobistego, należy również pamiętać o zastosowaniu odpowiednich środków technicznych i organizacyjnych w celu zapewnienia bezpieczeństwa przetwarzania danych osobowych. Rekomendowanym rozwiązaniem również jest wprowadzenie alternatywnych sposobów potwierdzenia tożsamości osoby składającej żądanie z zakresu ochrony danych osobowych, tak aby wnioskodawca miał możliwość dokonania wyboru, w jaki sposób chce się uwierzytelnić. Przy weryfikacji tożsamości w ramach usług świadczonych drogą elektroniczną można przykładowo wykorzystać możliwość podpisania dokumentu kwalifikowanym podpisem elektronicznym, podpisem profilem zaufanym ePUAP, podpisem osobistym w e-dowodzie czy też weryfikację tożsamości na podstawie tzw. przelewu weryfikacyjnego. W praktyce wykorzystywane są również inne rozwiązania, jak między innymi weryfikacja tożsamości podczas wideorozmowy, która stosowana jest zwykle przez podmioty objęte regulacjami ustawy o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu[6] (np. banki). Wspomniana ustawa zawiera odrębne regulacje dotyczące przetwarzania danych z dokumentu stwierdzającego tożsamość, jednakże ich szczegółowa analiza wymaga odrębnego opracowania.

[6] Ustawa z dnia 1 marca 2018 roku o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu.