Podpis biometryczny klienta na umowie

Posted on 2025-03-31

Każda decyzja administratora o pozyskiwaniu danych klienta opartych na biometrii powinna być poprzedzona szczególnie wnikliwą analizą. Przetwarzanie takich danych powinno się odbywać nie tylko z poszanowaniem zasady legalności, ale także być działaniem adekwatnym oraz stosownym i ograniczonym z punktu widzenia realizacji zakładanego celu. Jest to istotne tym bardziej, że w świetle art. 9 ust. 1 RODO zasadą jest zakaz przetwarzania takich danych, a odstępstwo od niego powinno mieć wyraźne oparcie w jednym z wyjątków wprost wymienionych w ust. 2 tego przepisu. Przesłanką legalizującą przetwarzanie takich danych mogłaby być więc np. zgoda klienta, o ile zostaną spełnione wszystkie określone w RODO warunki jej wyrażania.

W związku z rozwojem nowych technologii popularność na rynku zyskują długopisy cyfrowe. Umożliwiają one podpisanie umowy lub innego dokumentu własnoręcznym podpisem zapisywanym jednocześnie w formie cyfrowej. Dzięki wykorzystaniu takiego narzędzia możliwe jest powstawanie zarówno wersji papierowej dokumentów, jak i ich elektronicznych odpowiedników. Wątpliwości administratorów i inspektorów ochrony danych (IOD) budzi jednak kwestia kwalifikacji danych zbieranych przy tworzeniu cyfrowej wersji podpisu odręcznego. Czy takie dane należy uznać za dane biometryczne? Jak powinno wyglądać pozyskiwanie i wycofywanie zgody na ich przetwarzanie? Jakie środki ich ochrony przyjąć?

Kiedy cyfrowy podpis to dane biometryczne?

Wyjaśniając te wątpliwości, w pierwszej kolejności pod uwagę należy wziąć definicję danych biometrycznych zawartą w art. 4 ust. 14 RODO. Stanowi on, że dane te oznaczają „dane osobowe, które wynikają ze specjalnego przetwarzania technicznego, dotyczą cech (…) behawioralnych osoby fizycznej oraz umożliwiają lub potwierdzają jednoznaczną identyfikację tej osoby.” Europejska Rada Ochrony Danych (EROD) w Wytycznych 3/2019 w sprawie przetwarzania danych osobowych przez urządzenia wideo wskazała, że aby uznać określone dane za dane biometryczne, pod uwagę należy wziąć trzy elementy:

- • charakter danych – dane dotyczą cech fizycznych, fizjologicznych lub behawioralnych osoby fizycznej,
- • środki i sposób przetwarzania – wynikają z użycia odpowiedniej technologii,
- • cel przetwarzania – dane muszą być przetwarzane w celu jednoznacznej identyfikacji osoby.

Ponadto Grupa Robocza Art. 29 w Opinii 3/2012 w sprawie zmian sytuacji w dziedzinie technologii biometrycznych zaznaczyła, że jedną z kategorii technik biometrycznych są techniki behawioralne, które obejmują mierzenie zachowania danej osoby na podstawie podpisu odręcznego. Dodano, że „typowymi cechami dynamicznymi mierzonymi przez system biometrii podpisu odręcznego (taki jak tablet graficzny) są: stopień nacisku, kąt nachylenia pisma, prędkość i przyśpieszenie narzędzia pisarskiego, kształt liter, kierunek pisma oraz inne niepowtarzalne cechy dynamiczne”. Zatem biorąc po uwagę powyższe wskazówki uznać należy, że podpis złożony przy pomocy cyfrowego długopisu, który odczytuje i zapisuje kształt pisma, siłę nacisku, czas zapisu oraz szybkość ruchu ręki składającego podpis, można uznać za „dane biometryczne” w rozumieniu art. 4 ust. 1 i art. 9

RODO, jeżeli administrator używa określonych środków technicznych umożliwiających jednoznaczne zidentyfikowanie osoby fizycznej.

Szczególny reżim

Należy też pamiętać, że stosownie do art. 9 ust. 1 RODO „dane biometryczne" należą do szczególnych kategorii danych osobowych, których przetwarzanie co do zasady jest zakazane. Odstępstwo od tego zakazu jest możliwe, o ile spełniony jest jeden z warunków określonych w art. 9 ust. 2 RODO. W przypadku relacji firmy z klientem w grę wchodzi przesłanka, o której mowa w art. 9 ust. 2 lit. a RODO, tj. „osoba, której dane dotyczą, wyraziła wyraźną zgodę na przetwarzanie tych danych osobowych w jednym lub kilku konkretnych celach, chyba że prawo Unii lub prawo państwa członkowskiego przewidują, iż osoba, której dane dotyczą, nie może uchylić zakazu,
o którym mowa w ust. 1." Ponadto motyw 51 RODO określa, że „dane osobowe, które z racji swego charakteru są szczególnie wrażliwe w świetle podstawowych praw i wolności, wymagają szczególnej ochrony, gdyż kontekst ich przetwarzania może powodować poważne ryzyko dla podstawowych praw i wolności". Z tego powodu techniczne i organizacyjne środki ochrony danych osobowych wprowadzone przez administratora muszą ograniczyć czynniki ryzyka dla ochrony praw i wolności jego klientów.

Potrzebna ocena skutków dla ochrony danych

W związku z tym administrator przed wprowadzeniem stosowania technologii cyfrowego długopisu powinien przeprowadzić ocenę skutków dla ochrony danych (tzw. Data Protection Impact Assessment). RODO (art. 35) ustanawia taki obowiązek w sytuacji, gdy „dany rodzaj

przetwarzania – w szczególności z użyciem nowych technologii – ze względu na swój charakter, zakres, kontekst i cele z dużym prawdopodobieństwem może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych”. Dodać należy, że polski organ nadzorczy „przetwarzanie danych biometrycznych wyłącznie w celu identyfikacji osoby fizycznej bądź w celu kontroli dostępu” wskazał jako jeden z rodzajów operacji wskazujących na potrzebę przeprowadzenia takiej oceny (patrz wykaz rodzajów operacji przetwarzania danych osobowych wymagających oceny skutków dla ochrony danych; (dostępny pod linkiem). Częścią takiej oceny (zgodnie z powołaną Opinią Grupy Roboczej 3/2012) powinna być analiza tego, czy technologia cyfrowego długopisu i związane z nią przetwarzanie danych biometrycznych są niezbędne do świadczenia określonej usługi, czy nie jest to tylko rozwiązanie najdogodniejsze lub najbardziej opłacalne dla administratora.

Właściwe zabezpieczenia

Po przeprowadzeniu oceny ryzyka, administrator jest zobowiązany do wprowadzenia odpowiednich środków bezpieczeństwa danych osobowych, odpowiadających stopniowi zagrożenia (art. 32 RODO). Administrator powinien rozważyć odpowiednio:

- • pseudonimizację i szyfrowanie danych osobowych,
- • zdolność do ciągłego zapewnienia poufności, integralności, dostępności i odporności systemów
  i usług przetwarzania,
- • zdolność do szybkiego przywrócenia dostępności danych osobowych i dostępu do nich w razie incydentu fizycznego lub technicznego,
- • regularne testowanie, mierzenie i ocenianie skuteczności środków technicznych i organizacyjnych mających zapewnić bezpieczeństwo przetwarzania.
  Grupa Robocza Art. 29 w Opinii 3/2012 oraz EROD w Wytycznych 3/2019, w celu zapewnienia wysokiego poziomu ochrony technicznej przy przetwarzaniu danych

biometrycznych, zalecają
m.in.:

- • wprowadzenie mechanizmu automatycznego usuwania danych, aby zapobiec zbyt długiemu okresowi przechowywania danych biometrycznych,
- • wprowadzenie systemów weryfikujących autentyczność podpisującego,
- • przechowywanie informacji biometrycznych w postaci zaszyfrowanej oraz w oddzielnej bazie danych,
- • kategoryzacje danych w trakcie ich przesyłania i przechowywania.

Co więcej, administrator powinien uwzględnić już w procesie projektowania wdrożenie odpowiednich środków technicznych i organizacyjnych oraz domyślną ochronę, które zapewnią odpowiednią ochronę praw i wolności podmiotów (tzw. privacy by design oraz privacy by default) (art. 25 RODO). Pomocne może być zaznajomienie się z Wytycznymi EROD 4/2019 dotyczącymi artykułu 25 uwzględniającego ochronę danych w fazie projektowania oraz domyślną ochronę danych (dostępne pod linkiem: https://www.edpb.europa.eu/system/files/2021-04/edpb_guidelines_201904_dataprotection_by_design_and_by_default_v2.0_pl.pdf.

Odpowiednie poinformowanie o zastosowaniu danych

biometrycznych

Poza tym Grupa Robocza Art. 29 w Opinii 3/2012 zwraca uwagę, iż przetwarzanie danych na podstawie zgody jest ważne, jeżeli podmiotowi, którego dane będą przetwarzane, udzielona została wystarczająca ilość informacji o zastosowaniu danych biometrycznych. Informacje te są opisane w art. 13 ust. 1 i 2 RODO. Ze względu na szczególny charakter danych biometrycznych, należy zwrócić uwagę na podanie okresu przechowywania danych osobowych oraz informacje o prawie do cofnięcia zgody na ich przetwarzanie. Administrator powinien mieć również na względzie zasady: minimalizacji, ograniczenia przechowywania, integralności i poufności danych (art. 5 RODO).

Warunki pozyskiwania zgody klientów

Należy podkreślić, że według art. 4 ust. 11 RODO, „zgoda" oznacza dobrowolne, konkretne, świadome i jednoznaczne okazanie woli, którym osoba, której dane dotyczą, w formie oświadczenia lub wyraźnego działania potwierdzającego, przyzwala na przetwarzanie jej danych osobowych, w tym danych biometrycznych. 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. Istotne jest, aby klient, udzielając zgody, znał jej zakres i cel i wiedział, na czym konkretnie będzie polegało przetwarzanie jego danych.

Powinna istnieć również alternatywna metoda, z której podmiot danych mógłby skorzystać w przypadku braku zgody na przetwarzanie danych biometrycznych, tak, aby nie zostać

pozbawionym możliwości skorzystania z konkretnej usługi. Należy więc rozważyć, czy klient ma możliwość zawarcia umowy także składając inny niż biometryczny rodzaj podpisu. Motyw 43 RODO stanowi, że „zgody nie uważa się za dobrowolną, jeżeli nie można jej wyrazić z osobna na różne operacje przetwarzania danych osobowych". W motywie 32 doprecyzowano, że „zgoda powinna dotyczyć wszystkich czynności przetwarzania dokonywanych w tym samym celu lub w tych samych celach. Jeżeli przetwarzanie służy różnym celom, potrzebna jest zgoda na wszystkie te cele."

Ponadto, Wytyczne EROD 5/2020 dotyczące zgody na mocy rozporządzenia 2016/679 (dostępne pod linkiem) stanowią, że „usługa może obejmować wiele operacji przetwarzania w więcej niż jednym celu. W takich przypadkach osobom, których dane dotyczą, powinna przysługiwać swoboda wyboru celu, który akceptują, zamiast obowiązku wyrażenia zgody na szereg celów przetwarzania. W danym przypadku zgodnie z RODO uzasadnione może być wyrażenie kilku zgód w celu rozpoczęcia oferowania usługi." W związku z tym, administrator powinien umożliwić osobie, której dane dotyczą, wyrażenie zgody/zgód na przetwarzanie danych osobowych, w tym danych biometrycznych, na dokładnie określone cele doprecyzowane w zależności od umowy.

Administrator powinien również pamiętać, że jeżeli chce przetwarzać dane osobowe w innym celu niż oznajmiono osobie, której dane dotyczą, musi poprosić o zgodę tej osoby na nowy cel albo znaleźć inną podstawę prawną zgodną z art. 6 lub art. 9 RODO. Co ważne, art. 7 ust. 4 RODO oraz Wytyczne 5/2020 podkreślają, że „łączenie zgody z akceptacją warunków lub uzależnianie wykonania umowy lub świadczenia usługi od uwzględnienia wniosku
o wyrażenie zgody na przetwarzanie danych osobowych, które nie jest konieczne w celu wykonania umowy lub świadczenia usługi", jest działaniem niepożądanym i podważającym dobrowolność zgody. Ponadto administrator, stosownie do art. 7 ust. 3 RODO, jest zobowiązany zapewnić, aby osoba, której dane są przetwarzane, mogła wycofać zgodę w dowolnym momencie oraz z taką samą łatwością, jak jej udzieliła. Administrator już w

momencie pozyskiwania danych osobowych ma także obowiązek poinformowania osoby o prawie do wycofania zgody oraz o tym, jak tego dokonać. Zobowiązuje go do tego art. 13 ust. 2 lit. c RODO. Co więcej, Wytyczne EROD 5/2020 precyzują, że wycofanie zgody nie powinno przynieść żadnych niekorzystnych konsekwencji dla osoby, której dane są przetwarzane.

Biometria w sektorze finansowym

Jednocześnie warto przypomnieć, że w Biuletynie UODO Nr 04/04/24 w materiale „Biometryczna weryfikacja tożsamości klientów usług płatniczych" omówiona została kwestia stosowania przez instytucje finansowe analizy behawioralnej (np. sposobu pisania na klawiaturze czy sposobu poruszania myszą komputera) i tworzenia na podstawie cech charakterystycznych dla danego użytkownika jego unikalnego profilu oraz późniejsze wykorzystywanie tych danych w celu uwierzytelniania klientów usług płatniczych, co w opinii przedstawicieli środowiska finansowego ma umożliwiać ograniczanie transakcji oszukańczych w płatnościach bezgotówkowych. W tekście tym UODO wskazał, że 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.