



Wrocław, dnia 8 sierpnia 2016 r.

OPINIA PRAWNA

dotycząca rozwiązania *Paperless Signature* pod kątem zgodności z przepisami prawa w zakresie zachowania wymogów „klasycznego” podpisu własnoręcznego wykorzystywanego do zachowania formy pisemnej.

AKTY PRAWNE

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, dalej jako Rozporządzenie eIDAS;
2. Kodeks cywilny w brzmieniu po nowelizacji wprowadzonej ustawą z dnia 10 lipca 2015 o zmianie ustawy – Kodeks cywilny, ustawy – Kodeks postępowania cywilnego oraz niektórych innych ustaw wchodząca w życie 8 września 2016, dalej jako ZmKC z 10.5.2015 r.;
3. Ustawa z dnia 29 sierpnia 1997 Prawo bankowe, dalej jako PrBank;
4. Rozporządzenie Rady Ministrów z dnia 26 października 2004 r. w sprawie sposobu tworzenia, utrwalania, przekazywania, przechowywania i zabezpieczania dokumentów związanych z czynnościami bankowymi, sporządzonych na elektronicznych nośnikach informacji, dalej jako RozpCzynBank;
5. Ustawa z dnia 29 sierpnia 1997 o ochronie danych osobowych, dalej jako UODO;
6. Rozporządzeniu Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych, dalej jako RozpDokDO;
7. 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), dalej jako RODO.

UWAGI OGÓLNE

Analizowane rozwiązanie *Paperless Signature* jest rozwiązaniem opartym o następującą konfigurację techniczną (konfiguracja *hardware-software*):

- 1) Komputer z systemem operacyjnym *Windows*, *Wacom LCD Signature PAD STU-530* z rysikiem oraz oprogramowaniem *SignDoc* – zestaw 1;
- 2) Tablet z systemem operacyjnym *Android*, matrycą elektromagnetyczną rejestrującą dane biometryczne, rysikiem oraz oprogramowaniem *Signatus* – zestaw 2;
- 3) Tablet z systemem operacyjnym *Android*, rysikiem rejestrującym dane biometryczne (np. nacisk) oraz oprogramowaniem *Signatus* – zestaw 3;

W skład *Paperless Signature* wchodzi również oprogramowanie *SignAlyze* służące do wyświetlania danych biometrycznych dotyczących składanego własnoręcznego podpisu, a także dokonywania analizy zgodności złożonego podpisu z wcześniej złożonym wzorem.

OPIS CECH ROZWIĄZANIA

System *Paperless Signature* jest jednym z modułów platformy *Billennium Paperless*. Podstawową cechą systemu jest możliwość rejestracji danych statycznych lub/i dynamicznych odręcznego podpisu elektronicznego (dane statyczne: dwuwymiarowy obraz podpisu; dane dynamiczne: czas, nacisk, szybkość i przyspieszenie podpisu). Aplikacja może funkcjonować niezależnie lub jako element niezależnej aplikacji (służąc do składania podpisu). Możliwa jest weryfikacja składanego podpisu z podpisem referencyjnym i uruchamianie „akcji” wynikowych, a także możliwość parametryzowania procentowego współczynnika zgodności składanego podpisu z podpisem referencyjnym.

Rozwiązanie daje możliwość wygenerowania podpisywanego dokumentu elektronicznego w systemach centralnych lub lokalnie na stacji klienckiej oraz umożliwia dostosowanie obecnych wzorców dokumentacji funkcjonującej w organizacji do procesu rejestracji odręcznego podpisu elektronicznego, a także

statycznego i dynamicznego osadzania pól do podpisu (np. w określonych w dokumencie miejscach), a nadto pozwala na integrację z repozytorium dokumentów elektronicznych. Do podpisywanego dokumentu można dołączyć dodatkowe dane takie jak: aktywne formularze, zdjęcia i obrazy, załączniki, komentarze i notatki, certyfikaty bezpieczeństwa stron trzecich, znacznik czasu. Transfer podpisu z urzędnika rejestrującego do dokumentu elektronicznego jest szyfrowany, a następnie integrowany za pomocą algorytmów kryptograficznych zapewniających integralność podpisywanego dokumentu, w taki sposób iż podpis jest „unikalny” tj. brak jest możliwości jego „wycięcia” i „wklejenia” do innego dokumentu (niniejsze twierdzenia wynikają z dokumentów przedłożonych do przygotowania opinii, jak również z implementacji normy ISO 32000-1:2008 w zakresie podpisywania dokumentów PDF).

Powyższe elementy systemu są wielce istotne dla określenia, czy złożony podpis odręczny stanowi podpis własnoręczny w znaczeniu polskiego prawa. Warty podkreślenia jest fakt, że tylko podpisy złożone z użyciem systemów, które spełnią opisane w niniejszej opinii wymagania mogą stanowić podstawę do uznania za równoważne z podpisem odręcznym.

W opinii autorów – odpowiedź na pytanie, czy opiniowany system spełnia wymogi umożliwiające uznanie złożenia odręcznego podpisu, jako odpowiadającemu złożeniu podpisu własnoręcznego w rozumieniu polskiego prawa, jest uzależnione od spełnienia poniżej omówionych wymogów.

DOKUMENT ELEKTRONICZNY

Począwszy od 1 lipca 2016 r. wchodzi w życie rozporządzenie eIDAS, a następnie 8 września 2016r. ZmKC z 10.5.2015 r. istotnie zmieniające pojęcie dokumentu, w tym dokumentu elektronicznego, a także postępowania dowodowego z ich wykorzystaniem. Inaczej będzie się także podchodziło do zachowania wymogu formy pisemnej.

a) Elementy dokumentu

Dotychczas w doktrynie, jak i orzecznictwie uznawano za dokument wyłącznie taki, który był sporządzony za pomocą znaków graficznych uporządkowanych w logiczny ciąg pojęć. Nowe definicje dokumentu, które wchodzi w życie w 2016r. (1 lipca rozporządzenie eIDAS, 8 września ZmKc z 10.5.2015 r.) ujednolicają to pojęcie i w pełni dopuszczają dokument elektroniczny.

Przez dokument (w znaczeniu k.c.) będzie się rozumiało: nośnik informacji umożliwiający zapoznanie się z jego treścią. Cytowana definicja znacznie rozszerza zakres tego pojęcia w stosunku do ugruntowanej doktryny i orzecznictwa, obejmując swoim zakresem także dokumenty będące multimediami, w tym zawierającymi obraz i dźwięk. Jest to konsekwencją wejścia w życie 1 lipca 2016r. definicji dokumentu elektronicznego z eIDAS zgodnie z którą dokumentem elektronicznym jest każda treść przechowywana w postaci elektronicznej, w szczególności tekst lub nagranie dźwiękowe, wizualne lub audiowizualne.

Z całą stanowczością należy uznać, że dokument sporządzony za pomocą systemu *Paperless Signature*, jest dokumentem w znaczeniu nowej definicji. Jest to dokument opierający się o tekst, odnośnie którego zastosowanie będą miały przepisy Tytułu VI Oddziału III Kodeksu postępowania cywilnego, ale w związku z możliwością dołączania do dokumentu filmów, zdjęć, multimediiów itd., zastosowanie będą miały także przepisy art. 308 KPC.

b) Utrwalenie treści

Dla skuteczności prawnej dokumentu utrwalenie powinno następować w sposób umożliwiający zachowanie i odtworzenie dokumentów w niezmienionej postaci, a także zapoznanie się z jego treścią. System *Paperless Signature* pozwala na utrwalenie dokumentu elektronicznego w sposób odpowiadający powyższym wymogom dzięki implementacji normy ISO 32000-1:2008 w zakresie standardu dokumentów PDF. Argumentem przemawiającym za systemem *Paperless Signature* jest zintegrowanie złożonego poprzez system podpisu własnoręcznego za pomocą algorytmów kryptograficznych zapewniając integralność podpisu z konkretnym dokumentem. Dodatkowo rejestrowany jest znacznik czasu oparty o zegar systemowy urządzenia, na którym złożono podpis. Warty rozważenia jest

możliwość integracji z usługą kwalifikowanego znakowania czasem, co umożliwiłoby uzyskanie tzw. daty pewnej.

c) Zawarcie informacji w dokumencie

Dokument musi posiadać treść. Dokument elektroniczny sporządzony i opatrzony podpisem odręcznym nie odbiega w tym zakresie od dokumentu tradycyjnego. System *Paperless Signature* pozwala na wypełnienie tego wymogu. Podpisywany dokument może być generowany w systemach centralnych lub lokalnie na stacji klienckiej. Dla wypełnienia wskazywanej cechy dokumentu konieczna jest możliwość wyświetlenia jego treści, w sposób umożliwiający zapoznanie się z nią przed podpisaniem. Powinno to następować na lokalnej stacji klienckiej. Niedopuszczalnym jest podpisywanie dokumentu „w ciemno” bez jego wizualizacji, wyłącznie poprzez składanie podpisu w polu do podpisu. Zastosowane w systemie *Paperless Signature* rozwiązanie polegające na wizualizacji treści podpisywanego dokumentu na monitorze komputera (zestaw 1) czy na wyświetlaczu tabletu (zestawy 2 i 3) spełnia powyższe wymaganie.

d) Nośnik jako element dokumentu

Kolejnym koniecznym elementem dokumentu jest nośnik, na którym zostanie utrwalona informacja mająca znaczenie dowodowe w przypadku potencjalnego sporu przed sądem, bądź inną instytucją. Nowe ujęcie dokumentu w KC pozwala na uznanie za dokument utrwaloną informację zarówno na trwałym nośniku, takim jak twardy dysk, czy też inna pamięć trwała jednostki klienckiej, ale także zapis w chmurze. „Nie ma bowiem, w ujęciu nowych przepisów, wymogu (dla spełnienia definicji dokumentu) zapisywania dokumentu na nośniku, nad którym fizyczne władztwo lub w którego posiadaniu jest dysponent zapisywanej informacji. Dla skutecznego jej uznania za dokument, konieczne jest zapisanie tak by było możliwe odtworzenie. Przepisy nie wymagają, ani też nie odnoszą się do kwestii własności nośnika, na którym zapisywana jest informacja stanowiąca dokument. Nośnik może być własnością zarówno dysponenta dokumentu, jak także osoby trzeciej. Zapis więc w chmurze w sposób umożliwiający odtworzenie dokumentu, spełnia przesłanki definicji dokumentu” (D. Szostek [w:] *Informatyzacja postępowania cywilnego. Komentarz*, Warszawa 2016r., str. 76.).

e) Chmura jako nośnik

Dotychczasowe ujęcie dokumentu wskazywało, iż powinien on stanowić jedną całość (kartkę papieru, plik itd.). Nowa definicja legalna dokumentu elektronicznego sypizowana w rozporządzeniu eIDAS pozwala za taki uznać informację zapisaną w wielu miejscach na wielu nośnikach, byleby system zapewniał jego pełną integralność i umożliwiał zweryfikowanie jego autentyczności. Zapis dokumentu w chmurze obliczeniowej w wielu miejscach, na różnych nośnikach (serwerach) nie stanowi dyskwalifikacji takiego zapisu jako dokumentu w znaczeniu prawnym. Nie jest to zatem przeszkodą w traktowaniu takiego zapisu jako dokumentu.

f) Uwagi w przedmiocie ryzyka procesowego

Należy jednak mieć na uwadze, że istnieje brak wiedzy po stronie prawników, w tym sędziów odnośnie wyżej wymienionych kwestii, co może powodować konieczność wyjaśniania przedmiotowej problematyki w ewentualnym postępowaniu sądowym i przedstawiania odpowiednich w tym zakresie ekspertyz. Taki bowiem zapis, mocno odbiega od tego, z czym mają zazwyczaj do czynienia prawnicy. Należy uwzględnić nowy art. 254 §2¹ k.p.c., zgodnie z którym w razie potrzeby sąd może wezwać wystawcę dokumentu sporządzonego w postaci elektronicznej do udostępnienia informatycznego nośnika danych, na którym został zapisany.

SYSTEM *PAPERLESS SIGNATURE* A INTEGRALNOŚĆ DOKUMENTU

Dla wywołania skutku prawnego dokumentu w postaci elektronicznej, konieczne jest zapewnienie możliwości kontroli integracji warstwy dokumentu sporządzonej własnoręcznie (złożenia podpisu) oraz elektronicznie.

W dokumencie „*Paperless Signature – Bezpieczeństwo*” datowanym na 15 kwietnia 2016 r. przedstawiono mechanizm służący zapewnieniu integralności przetwarzanych dokumentów oraz zabezpieczeniu danych biometrycznych przy użyciu kryptografii asymetrycznej oraz funkcji skrótów.

PODPIS NA CZYTNIKU ELEKTRONICZNYM JAKO ELEMENT KONSTITUTYWNY DOKUMENTU

Jednym z elementów dokumentów, w szczególności w przypadku składania oświadczeń woli, jest podpis składającego oświadczenie. Podpis sam w sobie nie zawsze jest koniecznym elementem dokumentu (np. faktura nie wymaga podpisu, a jest powszechnie uznawana za dokument). W przypadku jednak, gdy wymagana jest forma pisemna lub przepisy wymagają złożenia podpisu na dokumencie – wówczas jest on konieczny.

a) Podpis w systemie *Paperless Signature*

W systemie *Paperless Signature* podpis jest składany za pomocą urządzeń specjalizacyjnych *Wacom*, tablety wyposażone w matrycę elektromagnetyczną a także tablety bez matrycy elektromagnetycznej, wyposażone dodatkowo w pióro rejestrujące część danych dynamicznych.

b) Wymogi formy pisemnej

Dla spełnienia wymogów formy pisemnej z art. 78 § 1 KC oświadczenie woli powinno być sporządzone w postaci tekstu (maszynowo lub w całości ręcznie), a następnie podpisane. W doktrynie, jak i orzecznictwie uznaje się, iż w formie pisemnej jest tylko ta część oświadczenia, która znajduje się nad podpisem. Inaczej ujmując ta część oświadczenia jaka została objęta zakresem podpisu. W tym miejscu należy podkreślić wagę umiejscowienia odpowiednich pól dla podpisu wykonywanego odręcznie na dokumentach elektronicznych. Uwzględniając zmiany wprowadzane do KC oraz eIDAS, a także brzmienie art. 78 § 1 KC zgodnie z którym do zachowania pisemnej formy czynności prawnej wystarcza złożenie własnoręcznego podpisu na dokumencie obejmującym treść oświadczenia woli, wydaje się dopuszczalne złożenie tego oświadczenia woli w postaci multimedialnej (nagranie audio-wideo), a następnie podpisanie. Problem jednakże w tym, iż tak złożony podpis własnoręczny musiałby być dołączony w odrębnym dokumencie, co naruszałoby zasadę integralności dokumentu, a także w sposób istotny jest

odmiennym sposobem zachowania formy pisemnej od dotychczasowego, co może powodować poważną barierę mentalną.

W doktrynie wskazuje się na dopuszczalność, iż w przypadku złożenia podpisu w odpowiedniej rubryce dokumentu (polu podpisu), z czym mamy bardzo często do czynienia w formularzach, złożony podpis należy traktować jako złożony do całości oświadczenia. Konieczne jest jednak intelektualne i przestrzenne powiązanie podpisu i podpisywanej treści. Za dopuszczalne należy uznać, iż pole podpisu może znajdować się na odrębnym urządzeniu (czytniku do składania odręcznego podpisu).

System *Paperless Signature*, umożliwia integrację odręcznego podpisu z dokumentem elektronicznym. Dla spełnienia omawianej przesłanki podpisu, konieczna jest jednakże możliwość uprzedniego zapoznania się podpisującego z podpisywaną treścią. Przykładem jest wyświetlenie treści informacji, z którą podpisujący może się zapoznać, bezpośrednio nad polem do złożenia podpisu lub bezpośrednio przed jego złożeniem. W ten sposób składający podpis będzie miał pewność, że oświadczenie przez niego składane jest integralne. Sugeruje się także możliwość zweryfikowania złożonego podpisu w podpisanym dokumencie, a następnie potwierdzenie w postaci elektronicznej takiego dokumentu, poprzez wykorzystanie kwalifikowanego podpisu elektronicznego lub kwalifikowanej pieczęci elektronicznej. Sugestia ta tyczy się oczywiście *expressis verbis* formy pisemnej tak, aby zapewnić jak najwyższy poziom "bezpieczeństwa" dowodowego.

d) Podpis jako element konieczny formy pisemnej

Koniecznym elementem formy pisemnej z art. 78 § 1 KC jest własnoręczny podpis. Wykładnia semantyczna wskazuje, iż jest to napisany własnoręcznie znak umożliwiający identyfikację podpisującego się i musi posiadać cechę trwałości. Przepisy nie przesądzają, iż musi to być długopis, pióro, czy też inne tradycyjne narzędzie do składania podpisów. Konieczne jest, by trwałość podpisu została zachowana, a utrwalenie powinno być takiego stopnia, aby bez zastosowania specjalnych zabiegów, po złożeniu podpisu, nie mógł on ulec zniszczeniu lub zatarciu w dłuższym okresie czasu. Niezmiernie istotnym jest także, aby zapewnić stan niemożliwości „przeniesienia” podpisu wraz z cechami behawioralnymi do innego dokumentu.

Ograniczenia przenoszalności podpisów z jednego dokumentu elektronicznego na inny dokument realizowane są przez algorytm opisany w dokumencie „*Paperless Signature – Bezpieczeństwo*” datowanym na 2016-04-15. Do cyfrowego podpisywania dokumentów niezbędna jest para kluczy – prywatny i publiczny. Po wykonaniu odręcznego podpisu elektronicznego na urządzeniu (pad, tablet) dane biometryczne podpisu są szyfrowane przy wykorzystaniu posiadanego przez użytkownika klucza publicznego. Klucz prywatny, który może w przyszłości posłużyć do odszyfrowania danych biometrycznych (np. w celu porównania ich z podpisem referencyjnym) zostaje przekazany zaufanej trzeciej stronie lub jest bezpiecznie przechowywany. Tak zaszyfrowane dane biometryczne zostają dołączone do dokumentu, a następnie przy wykorzystaniu algorytmu SHA-1 otrzymywany jest pierwszy skrót dokumentu. Skrót służy do weryfikacji dowolnie dużego zbioru danych. W przypadku ochrony przed modyfikacjami dokumentu (nawet najmniejszej), jest to suma kontrolna. Skrót wygenerowany w ten sposób jest szyfrowany za pomocą nowego, wygenerowanego klucza prywatnego, a następnie zaszyfrowany skrót oraz klucz publiczny są umieszczane w dokumencie. W celu zapewnienia integralności dokumentu z pierwszego skrótu dokumentu i danych biometrycznych wyliczany jest drugi skrót dokumentu, który jest umieszczany w dokumencie. Dokument jest zapisywany, a drugi klucz prywatny jest usuwany. Zastosowanie takiej kombinacji funkcji skrótu i szyfrowania zapewnia integralność, autentyczność oraz identyfikację podpisującego przy jednoczesnej ochronie danych biometrycznych przed powieleniem.

e) Podpis - pojęcie i elementy

Podpisem jest charakterystyczny dla danej osoby znak potwierdzający, pochodzącą od niego treść (sporządzoną przez tę osobę lub zaakceptowaną), trwale zapisaną na nośniku. Podpis będąc znakiem posiada podwójną strukturę: materialną (fizyczną postać znaku) oraz niematerialną (poznawcze znaczenie znaku). Podpis jest tym, co wskazuje autora, poświadcza autentyczność, chroni przed fałszerstwem, skłania do ostrożności, wymaga zastanowienia, gwarantuje wiarygodność, nadaje powagę, a także umożliwia identyfikację podpisującego się.

Sposób składania oświadczenia woli wpisuje się w definicję dynamiczną podpisu (sposób jego wytworzenia), natomiast funkcje w definicję funkcjonalną (tak. J. Janowski, Podpis elektroniczny w obrocie prawnym, Warszawa 2007, str. 28). Ta

pierwsza ulega ciągłej zmianie (system *Paperless Signature* wpisuje się w te zmiany), druga jest stała i niezmienna.

Podpis jest sposobem powiązania oświadczenia z osobą je składającą. Powiązanie to może być faktyczne (fizyczne), w tym manualne (naniesienie odręcznych znaków), oraz biometryczne (umożliwiające analizę cech fizjologicznych lub fizjonomicznych). „Określenie indywidualnych cech charakteru pisma bywa określane jako materialne odbicie funkcjonalno-dynamicznego kompleksu pisma. Określenie indywidualnych cech charakteru pisma odbywa się głównie przez analizę tzw. grafizmu pisma, który współtworzą m.in. takie elementy jak wielkość i stopień nachylenia poszczególnych znaków, siła nacisku pisma czy sposób położenia liter” (A. Koziczak, *Obraz graficzny podpisów składanych seryjnie* [w:] T. Widło *Wokół problematyki dokumentu. Księga pamiątkowa dedykowana Profesorowi Antoniemu Felusowi, Katowice 2005, str. 48 i nast.*).

f) Odręczny podpis elektroniczny

Akwizycja podpisu własnoręcznego przy użyciu urządzeń kompatybilnych z systemem *Paperless Signature*, a zgodnych z załącznikiem B do normy ISO/IEC 19794-7:2014 pozwala na przeprowadzenie badania, które odpowiada badaniu grafologicznemu, o jakości przewyższającej te bazujące na podpisie wykonanym na papierze. Na potwierdzenie tej tezy można przytoczyć okoliczność, że od ponad dwóch lat w ramach systemu Elektronicznego Potwierdzenie Odbioru Ministerstwa Sprawiedliwości odbiór przesyłek sądowych potwierdzany jest podpisem na kompatybilnych z przedstawionymi urządzeniami i nie doszło do podważenia autentyczności złożonego w ten sposób podpisu.

Oznacza to, iż podpis własnoręczny nie powstaje wskutek zastosowania określonej technologii, lecz jest właściwością danej osoby i powstaje w sposób naturalny. Składanie podpisu za pomocą systemu *Paperless Signature* wymaga odpowiedniego oprogramowania, jednakże nie do złożenia podpisu, ale do jego zachowania, utrwalenia, zintegrowania z treścią oświadczenia, a także zachowania wszystkich wymaganych funkcji podpisu. Dla zapewnienia odpowiednich domniemań powiązanych z podpisywanym dokumentem elektronicznym sugeruje się dostosowanie do systemu *Paperless Signature* usług zaufania w rozumieniu

rozporządzenia eIDAS, a w szczególności kwalifikowanego podpisu elektronicznego.

FORMA DOKUMENTOWA

Nowelizacja ZmKC z 10.5.2015 r. wprowadza nową formę czynności prawnych, tzw. "formę dokumentową". Zgodnie z nowym art. 77² KC dla zachowania formy dokumentowej wystarczy złożenie oświadczenia w postaci dokumentu, w sposób umożliwiający ustalenie osoby składającej oświadczenie.

Jest to jedna z najczęściej stosowanych form oświadczeń woli (praktycznie cała komunikacja elektroniczna), chociaż do tej pory była nieuregulowana.

W założeniu prawodawcy, forma dokumentowa w niektórych przypadkach ma zastąpić formę pisemną, liberalizując w ten sposób nadmierny rygoryzm prawny, a ponadto stworzyć ramy dla funkcjonowania formy, która obecnie jest już w obrocie powszechnie stosowana, a z uwagi na coraz bardziej dynamiczny rozwój nowych technologii, stale zyskuje na znaczeniu (np. e-maile lub SMSy).

Jest to forma pośrednia pomiędzy pisemną lub elektroniczną (obie te formy niosą za sobą duży rygoryzm prawny) a wypowiedzią ustną (zaliczaną w doktrynie do formy ustnej). Forma dokumentowa ujmuje w swoim zakresie bardziej ulotne i mniej pewne postaci oświadczeń, takie jak poczta elektroniczna, czy post na forum internetowym, które to postaci oświadczeń pozwalają (przynajmniej z pewną dozą prawdopodobieństwa lub pośrednio) na identyfikację składającego oświadczenie woli. Należy podkreślić, że oświadczenie złożone w formie dokumentowej jest mniej pewne niż te złożone w innych formach szczególnych.

Złożenie podpisu odręcznego w dokumencie elektronicznym (także nie spełniającego wszystkich funkcji podpisu własnoręcznego) w ramach systemu *Paperless Signature* wypełnia wymogi formy dokumentowej. Złożenie podpisu własnoręcznego pozwala za pomocą danych biometrycznych na zidentyfikowanie składającego oświadczenie, pod warunkiem iż dane go identyfikujące (imię i nazwisko itd.) zawarte są w dokumencie.

POSTAĆ ELEKTRONICZNA DLA CZYNNOŚCI BANKOWYCH

Zgodnie z art. 7 ust. 1 PrBank oświadczenia woli związane z dokonywaniem czynności bankowych mogą być składane w postaci elektronicznej. Literalne

brzmienie przedmiotowego przepisu wykazuje wprost, że prawodawca w celu uproszczenia obrotu dopuścił składanie oświadczeń woli w postaci elektronicznej. Ważne jest tutaj sformułowanie "postać elektroniczna", gdyż nie powinna być ona utożsamiana z formą elektroniczną stypizowaną w art. 78¹ KC po wejściu w życie ZmKC z 10.5.2015 r.

Co więcej, w art. 7 ust. 3 PrBank prawodawca uznaje, że nawet jeżeli ustawa zastrzega dla czynności prawnej formę pisemną, uznaje się, że czynność bankowa dokonana w postaci elektronicznej, spełnia wymagania formy pisemnej także wtedy, gdy forma została zastrzeżona pod rygorem nieważności. A zatem skutek złożenia oświadczenia woli w tej postaci jest równoznaczny z zachowaniem formy pisemnej, nawet jeśli ustawa przewiduje rygor nieważności (tak postanowienie Sądu Najwyższego z 11.3.2004 r., sygn. V CZ 12/04).

W doktrynie dostrzeżono pewną dozę niebezpieczeństwa, którą powoduje tak daleko idące rozluźnienie wymogów dotyczących formy, niemniej skutek w postaci ułatwienia dokonywania bankowych czynności prawnych przeważa.

Aby ograniczyć niebezpieczeństwo związane z liberalizacją formy czynności prawnej, prawodawca w RozpCzynBank uznał, że zastosowanie powinny mieć podpisy elektroniczne.

Zgodnie z par. 4 RozpCzynBank, utworzenie dokumentu polega na zapisaniu sekwencji danych, związanych z jedną lub wieloma czynnościami bankowymi, na elektronicznym nośniku informacji i podpisaniu tych danych. Paragraf 3 RozpCzynBank stanowi natomiast, że ilekroć mowa o podpisaniu, należy przez to rozumieć złożenie bezpiecznego podpisu elektronicznego, złożenie podpisu elektronicznego, lub dołączenie danych identyfikujących, zgodnie z umową stron, a w przypadku dokumentów wewnętrznych banku - zgodnie z jego uregulowaniami wewnętrznymi.

W art. 7 ust. 2 PrBank ustawodawca zalegalizował możliwość zastąpienia dokumentacji papierowej elektroniczną. Z przepisu wynika, że dotyczy to wszelkich dokumentów związanych z czynnościami bankowymi. Mogą one być zapisane na informatycznych nośnikach danych, których funkcją jest magazynowanie informacji w postaci elektronicznej tj. np. płyty CD, pendrive'y, chmury obliczeniowe.

Warunkiem, który ustanowił prawodawca, aby prowadzić dokumentację w postaci elektronicznej jest jej należyte utworzenie, utrwalanie, przekazanie, przechowywanie i zabezpieczanie. Brak spełnienia któregokolwiek z tych wymogów powoduje, że bankowa dokumentacja elektroniczna nie będzie spełniała wymogów formy pisemnej. Bank naruszający wymogi określone w art. 7 ust. 2 PrBank w zakresie dokumentacji związanej z dokonywaniem czynności bankowych może narazić się również na sankcje ze strony Komisji Nadzoru Finansowego (art. 138 PrBank).

Ustawodawca dopuszcza wykonywanie usług związanych z zabezpieczeniem dokumentów związanych z dokonywanymi przez bank czynnościami również podmiotom spoza banku – spółkom tworzonym przez banki z innymi podmiotami, a także przedsiębiorstwom pomocniczych usług bankowych.

Zestawiając powyższe rozważania prawne z technicznymi możliwościami Systemu *Paperless Signature*, należy uznać, że wypełnia on wymogi postaci elektronicznej czynności bankowych, o której mowa w art. 7 PrBank.

WARUNKI TECHNICZNE PRZETWARZANIA DANYCH OSOBOWYCH

Zgodnie z UODO zabezpieczenie danych w systemie informatycznym polega na wdrożeniu i eksploatacji stosownych środków technicznych i organizacyjnych zapewniających ochronę danych przed ich nieuprawnionym przetwarzaniem.

Na podstawie art. 36 UODO Administrator danych jest obowiązany zastosować środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych odpowiednią do zagrożeń oraz kategorii danych objętych ochroną, a w szczególności powinien zabezpieczyć dane przed ich udostępnieniem osobom nieupoważnionym, zabranieniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ustawy oraz zmianą, utratą, uszkodzeniem lub zniszczeniem. Administrator danych prowadzi dokumentację opisującą sposób przetwarzania danych oraz środki, o których mowa w ust. 1.

W RozpDokDO na administratora danych osobowych nakłada się obowiązek stosowania wysokiego poziomu bezpieczeństwa przetwarzania danych osobowych w systemie informatycznym, gdy przynajmniej jedno urządzenie systemu

informatycznego, służącego do przetwarzania danych osobowych, połączone jest z siecią publiczną.

Zważywszy na treść przedstawionej do opinii dokumentacji, należy wysnuć wniosek, iż w rozwiązaniu *Paperless Signature* stosowane są środki bezpieczeństwa na poziomie wysokim, przez co system spełnia wymogi ochrony danych osobowych sypizowane w UODO oraz RozpDokDO. Opiniowany system umożliwia przechowywanie danych bezpośrednio przez beneficjenta lub przez podmiot trzeci. Dla określenia, czy dane wytworzone w ramach *Paperless Signature* są odpowiednio przechowywane konieczna jest kompleksowa analiza dotycząca przechowywania danych, dokumentacji z tym związanej itd., co jest możliwe w odniesieniu do konkretnych wdrożeń.

Niestety nie jest możliwe *a priori* uznanie, że wdrożony system *Paperless Signature* będzie zawsze spełniał wymogi ochrony danych osobowych zważywszy na okoliczność możliwości przetwarzania danych osobowych w sposób niezgodny z prawem przez podmiot, który wdroży system *Paperless Signature*. Podczas wdrożenia systemu *Paperless Signature*, aby zapewnić zgodność z UODO oraz RODO, należy dokonać analizy prawnej projektu wdrożeniowego oraz zasad obiegu danych w ramach systemu, a także ich przechowywania. Pomimo, że system *Paperless Signature* spełnia techniczne wymogi ochrony danych osobowych, to nieprawidłowe wdrożenie systemu może doprowadzić do potencjalnego naruszenia zasad prywatności i ochrony danych osobowych.

Ze względu na uchwalenie RODO należy podkreślić, że wdrożenie rozwiązania *Paperless Signature* będzie musiało zostać dostosowane w aspekcie prawnym (nie technicznym) do jego wymogów. Wybranymi istotnymi zmianami będzie uznanie danych biometrycznych za dane osobowe, a także obowiązek wdrożenia zasad *privacy by default* oraz *privacy by design*. Zasady te wymuszają na wszystkich administratorach danych obowiązek uwzględnienia ochrony danych osobowych i prywatności na każdym etapie projektowania, tworzenia, a także funkcjonowania systemów i technologii obejmujących przetwarzanie danych osobowych. Zasady ochrony danych osobowych powinny tym samym być zaimplementowane w każdy projekt już na etapie jego założeń. Przetwarzanie danych osobowych powinno następować w taki sposób, aby ochrona prywatności osób fizycznych stanowiła jego immanentną i nieodłączną część. Ponadto RODO wymaga, aby system

przetwarzający dane osobowe, w ustawieniach domyślnych, tj. zdefiniowanych automatycznie, udostępniał jak najmniejszą ilość informacji o osobie korzystającej z systemu. Jedynie w takim zakresie, jaki jest wymagany do poprawnego jego użytkowania. Zwiększenie zakresu przetwarzanych danych będzie mogło nastąpić jedynie w następstwie zmian w ustawieniach wprowadzonych przez użytkownika. Rozporządzenie zacznie obowiązywać w pierwszej połowie 2018 r. i wtedy też zasady te powinny zostać wdrożone.

WNIOSKI

System *Paperless Signature* w przypadku spełnienia powyżej omówionych przesłanek, przede wszystkim związanych z realizacją wszystkich funkcji podpisu własnoręcznego (powiązania oświadczenia z osobą je składającą), integralności treści oświadczenia w dokumencie elektronicznym oraz złożonego podpisu, a także zapewnienia autentyczności pozwala w ocenie autorów zakwalifikować odręczny podpis za złożenie oświadczenia w formie pisemnej.

System *Paperless Signature* może wypełniać obowiązki w zakresie ochrony danych osobowych na gruncie technicznym, niemniej podczas jego każdorazowego wdrażania należy mieć na uwadze zapewnienie zgodności z prawem zasad przetwarzania danych osobowych.

Bez najmniejszych wątpliwości złożony odręcznie podpis własnoręczny jest podpisem elektronicznym w znaczeniu art. 3 pkt. 10 rozporządzenia eIDAS, czyli danymi w postaci elektronicznej dołączonymi lub logicznie powiązanimi z innymi danymi w postaci elektronicznej i które użyte są przez podpisującego jako podpis. Takim narzędziem jest każdy własnoręczny podpis złożony w systemie *Paperless Signature*. Natomiast odręczny podpis w dokumencie elektronicznym (składany przy użyciu systemu *Paperless Signature*) spełniający wszystkie funkcje podpisu własnoręcznego, poprzez wprowadzenie nowej definicji dokumentu, w ocenie opiniujących pozwala na uznanie takiego podpisu za własnoręczny, spełniający wymogi zachowania formy pisemnej. Jest to zerwanie z dotychczasowym ujęciem i rozumieniem podpisu własnoręcznego, dlatego też wymaga ono zmiany mentalnościowej zarówno w społeczeństwie, jak i wśród prawników, w tym sędziów, a także naukowców. Do tej pory nie uważano bowiem, żeby podpis w dokumencie elektronicznym można było uznawać za podpis własnoręczny. Należy spodziewać się oporu przed takim ujęciem zagadnienia i prób odmiennych argumentacji. Tradycyjny podpis własnoręczny jest tak silnie powiązany mentalnie z tradycyjnym jego ujęciem i dokumentem papierowym, iż należy spodziewać się trudności (przynajmniej na pierwszym etapie) w pozytywnej interpretacji większości praktyków. Jednakże w opinii przygotowującego ekspertyzę byłby to

podpis własnoręczny w dokumencie elektronicznym, zachowujący wymagania formy pisemnej. Takie rozwiązanie przełamuje utarte schematy, ale też bez dodatkowych zabiegów legislacyjnych może być używane we wszystkich przypadkach, gdzie jest wymagana forma pisemna (czy ze względów materialnoprawnych, czy też procesowych).

Sporządzający opinię:

prof. n. dr hab., radca prawny Dariusz Szostek - partner zarządzający Szostek_Bar i Partnerzy

mgr. inż. Krzysztof Kamiński - Dyrektor działu IT Szostek_Bar i Partnerzy

