

UWAGI

**Polskiej Izby Informatyki i Telekomunikacji [PIIT]
do projektu rozporządzenia Rady Ministrów w sprawie sposobu tworzenia, utrwalania,
przekazywania, przechowywania i zabezpieczania dokumentów związanych z czynnościami
bankowymi, sporządzanych na informatycznych nośnikach danych**

Uwaga 1 - ogólna

Zgodnie z intencją wyrażoną w opisie potrzeby zmian ww. Rozporządzenia czytamy:

*Zgodnie z art. 7 ust. 1-3 ustawy z dnia 29 sierpnia 1997 r. – Prawo bankowe, oświadczenia woli związane z dokonywaniem czynności bankowych mogą być składane w postaci elektronicznej, a dokumenty związane z czynnościami bankowymi mogą być sporządzane na informatycznych nośnikach danych, jeżeli dokumenty te będą w sposób należyty utworzone, utrwalone, przekazane, przechowywane i zabezpieczone, co zapewnia bank. Jeżeli ww. ustawa zastrzega dla czynności prawnej formę pisemną, uznaje się, że czynność dokonana w formie „elektronicznej” spełnia wymagania formy pisemnej także wtedy, gdy forma została zastrzeżona pod rygorem nieważności. Na podstawie art. 7 ust. 4 ustawy z dnia 29 sierpnia 1997 r. – Prawo bankowe wydano rozporządzenie Rady Ministrów z dnia 26 października 2004 r. w sprawie sposobu tworzenia, utrwalania, przekazywania, przechowywania i zabezpieczania dokumentów związanych z czynnościami bankowymi, sporządzanych na elektronicznych nośnikach informacji (Dz. U. poz. 2364). **W wyniku wejścia w życie rozporządzenia eIDAS, wystąpiła konieczność wydania nowego rozporządzenia, które będzie stosowało terminologię odnoszącą się do podpisów elektronicznych zgodnie z rozporządzeniem eIDAS.***

Chcielibyśmy wskazać rozbieżność między ww. intencją, a finalną wersją zapisów definicyjnych, gdzie czytamy:

podpis elektroniczny – należy przez to rozumieć kwalifikowany podpis elektroniczny albo inny podpis elektroniczny zgodny z umową stron, a w przypadku dokumentów wewnętrznych banku, zgodny z jego przepisami wewnętrznymi;

Patrząc przez pryzmat uwag zgłoszonych wcześniej należy wskazać, że podpis w rozumieniu artykułu 7 Prawa Bankowego nie jest podpisem w rozumieniu eIDAS. Zgodnie z eIDAS, rozporządzenie jest stosowane tylko do usług zaufania i usług identyfikacji. Podpis „bankowy” nie jest realizowany w ramach usługi zaufania, a co za tym idzie nie może korzystać ze skutków prawnych rozporządzenia eIDAS.

W tym zakresie przyjęcie ww. propozycji definicyjnej, bez odesłania wprost do definicji eIDAS jest w rzeczywistości pominięciem prawa europejskiego.

Innymi słowy intencja wyrażona w we wstępie do Uwagi 1 nie pokrywa się z finalną wersją projektu zmiany Rozporządzenia w tym zakresie

Uwaga nr 2

Propozycja zapisu dla par. 5 punkty 5 i 6:

Jest:

5. Dokumenty mogą być kopiowane na inny informatyczny nośnik danych pod nadzorem osób, które zostały uprawnione zgodnie z przepisami wewnętrznymi banku, z zachowaniem zasad bezpieczeństwa obrotu oraz ochrony interesów banków i ich klientów.

6. Każdy informatyczny nośnik danych użyty do przechowywania dokumentów zawiera oznaczenie umożliwiające identyfikację tego nośnika (identyfikator).

Propozycja:

Par. 5 pkt 5. (do wykreślenia – patrz propozycja nowego brzmienia par. 4 poniżej)

Par. 5 pkt 6. (do wykreślenia – patrz propozycja dodania paragrafu po par. 7)

Propozycja zmiany brzmienia par. 4 z uzupełnieniem wynikającym z obecnego brzmienia par. 5 pkt 5

Jest:

§ 4. Dokument może być przekazany na informatycznym nośniku danych albo za pomocą środków komunikacji elektronicznej, w sposób zapewniający integralność przekazywanego dokumentu.

Propozycja:

§ 4. Dokument może być przekazany na informatycznym nośniku danych albo za pomocą środków komunikacji elektronicznej, w sposób zapewniający integralność przekazywanego dokumentu, z zachowaniem zasad bezpieczeństwa.

Uzasadnienie: kopiowanie z obecnego par. 5 pkt 5. jest równoważne z kopiowaniem z par. 4, a zatem można tylko rozszerzyć par. 4 o elementy związane z bezpieczeństwem. Proponujemy wykreślić nadzór osób, ponieważ część dokumentów może w sposób automatyczny być kopiowana do innych nośników (proces automatyczny). Proponujemy zastąpić „bezpieczeństwo obrotu” po prostu „bezpieczeństwem”. Proponujemy wykreślenie stwierdzenie „ochrony interesów banków i ich klientów” ze względu na oczywistość tego stwierdzenia.

Propozycja związana z wykreśleniem par. 5 pkt 6 i dopisania nowego paragrafu po par. 6

Uzasadnienie wykreślenia pkt. 6. Nie jest oczywiste czy projektodawca miał na myśli identyfikację informatyczną nośnika czy też oznaczenie fizycznego nośnika. W dzisiejszych technologiach to drugie może być wręcz kłopotliwe, drogie i czasochłonne (np. przy jakichkolwiek awariach nośnika), a eliminujące tanie i efektywne rozwiązania (np. usługi backupu). Również wymagania zapisane w pkt. 1-3 czynią punkt 6 nadmiarowym i jedynie mnożącym koszty natomiast nie podwyższającym bezpieczeństwa.

Niech przykładem będzie sytuacja, w której awarii ulega jeden z dwóch nośników, na których zapisany jest dokument. W takiej sytuacji tym co trzeba zrobić najszybciej to stworzenie drugiej kopii, co w dzisiejszych systemach zostanie zrobione automatycznie. Natomiast zgodnie z duchem konsultowanej propozycji należy wykonać wiele innych czynności (zapewnić nadzór osób z uprawnieniami, oznaczyć nowy nośnik, itd. itp.) – w przypadku poważniejszej awarii lub ataku cybernetycznego może to oznaczać bezpowrotną utratę dokumentów!

Proponujemy następujący zapis:

Paragraf X (po paragrafie 6). Bank wykonujący czynności związane z dokumentami opisane w niniejszym rozporządzeniu musi być w stanie wykazać przestrzeganie przepisów („rozliczalność”).

Uzasadnienie: bank dokonujący operacji na dokumentach musi wykazać zgodność swoich działań z niniejszym rozporządzeniem (patrz analogiczne rozwiązanie prawne w art. 5.2. RODO), a zatem m.in. musi potrafić m.in. zidentyfikować gdzie znajdują się dokumenty, zapewnić ich integralność, usunięcie w sposób nieodwracalny, bezpieczeństwo itd. itp. – czyli zapisy par. 3-6. Natomiast nie narzuca to bankom konkretnych rozwiązań technicznych, które mogą się zmieniać w czasie i zgodnie z postępowaniem technologicznym. Bardzo podobny sposób rozumienia bezpieczeństwa reprezentuje ustawa o krajowym systemie cyberbezpieczeństwa (m.in. nakłada obowiązki audytowe i prowadzenia dokumentacji na operatorów usług kluczowych, wśród których oczywiście są także i banki). Proponowane rozwiązanie pozwoli wykorzystać procedury już istniejące bez mnożenia kosztów, a przy zachowaniu bezpieczeństwa przechowywania dokumentów.