

Ustawa Modelowa UNCITRAL o podpisach elektronicznych

Zgromadzenie Ogólne,

Przywołując rezolucję 2205 (XXI) z dnia 17 grudnia 1966 roku, która ustanowiło Komisje Międzynarodowego Prawa Handlowego ONZ, zlecając prowadzenie prac nad postępującą harmonizacją i unifikacją międzynarodowego prawa handlowego i w tym odniesieniu branie pod uwagę interesów wszystkich ludzi, a w szczególności tych z państw rozwijających się, ze względu na postępujący rozwój międzynarodowego handlu,

Zwracając uwagę, że wzrastająca ilość transakcji w handlu międzynarodowym dokonuje się za pośrednictwem środków komunikacji powszechnie uznawanych za handel elektroniczny, który wiąże się z wykorzystaniem alternatywnych do opartych na papierze form komunikacji, przechowywania i poswiadczenia informacji,

Przywołując rekomendacje o wartości prawnej zapisów komputerowych przyjęte przez Komisje w 1985 roku na osiemnastej sesji oraz ustęp 5 punkt (b) Rezolucji 40/71 Zgromadzenia Ogólnego z dnia 11 grudnia 1985 roku, w którym Zgromadzenie powołało Rady i organizacje międzynarodowe do podjęcia działań, gdzie konieczne, w zgodzie z rekomendacją Komisji tak, aby zapewnić bezpieczeństwo prawne w kontekście jak najszerszego możliwego użycia automatycznego przetwarzania danych w handlu międzynarodowym,

Przywołując również Prawo Modelowe o Handlu Elektronicznym, przyjęte przez Komisje na 29 sesji w 1996 roku, uzupełnione przez dodatkowy artykuł 5' przyjęty na 31 sesji w 1998 roku i ustęp 2 Rezolucji 51/162 Zgromadzenia Ogólnego z 16 grudnia 1996, w którym Zgromadzenie rekomenduje wszystkim Państwom, aby przychylnie rozwały Prawo Modelowe w tworzeniu lub zmianie własnego prawa, z uwagi na konieczność ujednoczenia praw stosowanych do alternatywnych do opartych na papierze metod komunikowania i przechowywania informacji,

Przekonani, że Prawo Modelowe o Handlu Elektronicznym jest doniosłą pomocą w umożliwianiu lub ułatwianiu stosowania handlu elektronicznego, co potwierdza wykorzystanie tego Prawa Modelowego do tworzenia ustawodawstwa w wielu państwach oraz uniwersalne jego stosowanie jako istotnego odnośnika w dziedzinie prawa handlu elektronicznego,

Dbając o doniosłą użyteczność nowych technologii, wykorzystywanych do identyfikacji osób w handlu elektronicznym i powszechnie odnoszących się do podpisu elektronicznego,

Zycząc sobie, aby stworzyć na podstawowych zasadach zakreślonych w artykule 7 Ustawy Modelowej o Handlu Elektronicznym, mając w perspektywie wypełnienia funkcji podpisu w środowisku elektronicznym, mając na względzie promowanie zaufania do podpisów elektronicznych dla osiągnięcia skutków prawnych, gdzie takie podpisy elektroniczne są funkcjonalnie równe podpisom odrecznym,

Przekonani, że pewność prawna w handlu elektronicznym będzie wzmocniona harmonizacją pewnych zasad prawnego uznawania podpisów elektronicznych opartych na zasadach technologicznej neutralności oraz stworzeniem metod oceny praktycznej niezawodności i handlowej adekwatności, na zasadach technologicznej neutralności,

Wierząc, że Ustawa Modelowa o Podpisach Elektronicznych stanowić będzie przydatne uzupełnienie Ustawy Modelowej o Handlu Elektronicznym i znacząco pomoże Państwom we wzmocnieniu ich ustawodawstwa, które rzadzi wykorzystaniem nowoczesnych technik potwierdzania autentyczności i w tworzeniu przepisów prawa w tej dziedzinie tam, gdzie jeszcze takie nie istnieją,

Bedąc zdania, że ustanowienie ustawy modelowej, aby ułatwić stosowanie podpisów elektronicznych w sposób akceptowalny przez Państwa o różnych systemach prawnych, społecznych i ekonomicznych, może również przyczynić się do rozwoju harmonijnych związków

ekonomicznych w handlu międzynarodowym,

1. Wyraża uznanie dla Komisji ONZ ds. Międzynarodowego Prawa Handlowego dla skompletowania i przyjęcia Prawa Modelowego o Podpisach Elektronicznych zawartego w załączniku do tej Rezolucji i za przygotowanie przewodnika do tworzenia prawa w oparciu o Prawo Modelowe;
2. Zaleca wszystkim Państwom, aby przychylnie rozważyły uwzględnienie Prawa Modelowego o Podpisach Elektronicznych i Prawa Modelowego o Handlu Elektronicznym, przyjętego w 1996 i uzupełnionego w 1998 roku, gdy będą tworzyły lub uzupełniały własne prawo, uwzględniając potrzeby ujednoczenia praw stosowanych do alternatywnych do opartych na papierze form komunikacji, przechowywania i potwierdzania autentyczności informacji;
3. Zaleca też, aby wszystkie starania do zapewnienia że Prawo Modelowe o Handlu Elektronicznym i Prawo Modelowe o Podpisach Elektronicznych, wraz z przewodnikami do tworzenia prawa stały się powszechnie znane i dostępne.

85 spotkanie plenarne

12 grudnia 2001 roku

Artykul 1. Zakres zastosowania

Ustawie stosuje sie do podpisów elektronicznych uzywanych w odniesieniu do czynnosci handlowych. Ustawa nie zmienia norm prawa, majacych na celu ochrone konsumentów.

Artykul 2 .Definicje

Dla celów tej ustawy:

- a) "Podpis elektroniczny" oznacza dane w formie elektronicznej dolaczone lub logicznie powiazane z przekazem danych, które moga byc uzyte do identyfikacji podpisujacego w zwiazku z przekazem danych oraz do oznaczenia aprobaty informacji zawartych przekazie danych;
- b) "Certyfikat" oznacza wiadomosc albo inny zapis potwierdzajacy zwiazek miedzy podpisujacym a danymi sluzacymi do stworzenia podpisu;
- c) "Przekaz danych" oznacza informacje wygenerowana, wyslana, otrzymana lub przechowywana za pomoca srodków elektronicznych, optycznych lub podobnych, w tym min. dane przesyłane elektronicznie (EDI), poczta elektroniczna, telegram, telex lub telekopiarka; bedaca aktem dzialania danej osoby albo pelnomocnika, wystepujacego w imieniu osoby, która reprezentuje;
- d) "Podpisujacy" ("Sygnatariusz") oznacza osobe, która posiada dane do tworzenia podpisu i dziala we własnym imieniu albo w imieniu osoby, która reprezentuje;
- e) "Dostawca uslug certyfikujacych" oznacza osobe, która wydaje certyfikaty i moze dostarczac innych uslug zwiazanych z podpisami elektronicznymi;
- f) "Osoba powiazana" oznacza osobe, która moze dzialac na podstawie certyfikatu lub podpisu elektronicznego.

Artykul 3. Równe traktowanie (różnych) technologii podpisu

Zaden przepis tej ustawy, poza artykulem 5 nie powinien byc stosowany w celu wylaczenia, ograniczenia albo pozbawienia skutków prawnych jakiegokolwiek metody tworzenia podpisu elektronicznego, która spelnia wymagania opisane w artykule 6, ustep 1, albo w przeciwnym razie, spelnia wymagania własciwego prawa.

Artykul 4. Interpretacja

- 1.Przy interpretacji tej ustawy nalezy miec na wzgledzie jego miedzynarodowy charakter i potrzebe promowania jednolitosci jego stosowania oraz poszanowanie dobrej wiary.
- 2.Kwestie mieszczace sie w zakresie kognicji tej ustawy, które nie zostaly bezposrednio uregulowane, powinny byc ustalone w oparciu o podstawowe zasady, na których ustawa jest oparta.

Artykul 5. Zmiany umowne

Przepisy ustawy moga zostac pozbawione swej mocy lub zmienione w drodze umowy, chyba ze umowa nie bedzie prawnie obowiazujaca lub skuteczna pod rzadami stosowanego prawa.

Artykul 6. Wypelnienie wymagan dla podpisu

- 1.W przypadkach, w których prawo wymaga podpisu osoby, wymaganie to jest spelnione dla przekazu danych, jesli uzyty podpis elektroniczny jest godny zaufania jako odpowiedni do celu, dla którego przekaz danych zostal stworzony lub przekazany, w swietle wszystkich okolicznosci, wlaczajac w to jakiegokolwiek stosowne porozumienie stron;
- 2.Ustep 1 ma zastosowanie, gdy wymagania tam opisane sa w formie zobowiazania lub gdy prawo

wyznacza bezpośrednio skutki braku podpisu;

3. Podpis elektroniczny jest uznawany za odpowiedni, by spełniał wymagania opisane w ustępie 1, jeśli:

- a) dane niezbędne do stworzenia podpisu elektronicznego w kontekście, do którego zostały użyte, są powiązane z podpisującym i z żadną inną osobą;
- b) dane niezbędne do stworzenia podpisu elektronicznego były w momencie zastosowania podpisu pod kontrolą podpisującego i żadnej innej osoby;
- c) jakkolwiek zmiana na podpisie elektronicznym uczyniona po momencie zastosowania podpisu jest możliwa do wykrycia;
- d) gdy celem prawnych wymogów dla podpisu elektronicznego jest gwarancja integralności informacji, do której dany podpis się odnosi, jakkolwiek zmiana dokonana na tej informacji po momencie zastosowania podpisu jest możliwa do wykrycia;

4. Ustęp 3 nie ogranicza zdolności jakiegokolwiek osoby do:

- a) ustalenia w jakikolwiek inny sposób, w celu spełnienia wymagań dla pewności podpisu elektronicznego, opisanych w ustępie 1; lub
- b) podania większej ilości dowodów na niezetelność podpisu elektronicznego,

5. Postanowienia tego artykułu nie mają zastosowania w następujących przypadkach: [...]

Artykuł 7. Spełnienie wymagań z artykułu 6

1. [Jakkolwiek osoba, organ, *urząd*, zarówno publiczny jak i prywatny, określony przez Państwo jako właściwy] może określić, który podpis elektroniczny spełnia wymagania zawarte w postanowieniach artykułu 6 tej ustawy.

2. Postanowienia przyjęte w ustępie 1 są zgodne z przyjętymi standardami międzynarodowymi.

3. Żadne z postanowień tego artykułu nie wywiera wpływa na działanie norm prawa prywatnego międzynarodowego.

Artykuł 8. Zachowanie sygnatariusza (podpisującego)

1. Gdy dane służące do stworzenia podpisu elektronicznego, mogą zostać wykorzystane do stworzenia podpisu wywierającego skutki prawne, każdy podpisujący:

- a) zachowuje należyta staranność w celu uniknięcia nieautoryzowanego użycia należących do niego danych niezbędnych do stworzenia podpisu elektronicznego;
- b) bez zbędnej zwłoki wykorzysta udostępnione przez dostawcę usług certyfikacyjnych środki na podstawie artykułu 9 tej ustawy albo w przeciwnym przypadku doloży wszelkich starań, by zawiadomić, kogokolwiek, kogo z uzasadnionych przyczyn podpisujący podejrzewa, że opiera się na podpisie elektronicznym lub dostarcza usług wspierających podpis elektroniczny, jeśli:
 - (i) podpisujący wie, że dane służące do stworzenia podpisu elektronicznego zostały przejęte; lub
 - (ii) okoliczności znane podpisującemu dają podstawę do zaistnienia poważnego ryzyka, że dane niezbędne do stworzenia podpisu elektronicznego mogły zostać przejęte;
- c) gdy certyfikat jest używany do wsparcia podpisu elektronicznego, dokłada należytej staranności, aby zapewnić dokładność i zupełność wszystkich istotnych upoważnień, wydanych przez podpisującego tak, że są relewantne do certyfikatu przez cały cykl jego ważności lub że są włączone do certyfikatu.

Artykuł 9. Zachowanie certyfikowanych dostawców usług

W przypadkach gdy dostawca usług certyfikacyjnych dostarcza usług wspierających podpis elektroniczny, który może zostać użyty dla wywołania skutków prawnych jako podpis, dostawca usług certyfikacyjnych powinien:

- (a) działać na podstawie upoważnień uzyskanych przez siebie w zgodzie ze stosowaną polityką i praktyką;
- (b) dochować należytej staranności, aby zapewnić dokładność (ściśłość) i zupełność wszystkich istotnych upoważnień, stworzonych przez siebie tak, aby były relewantne do certyfikatu przez cały cykl ważności albo żeby były włączone do certyfikatu;
- (c) dostarczać dostępnych środków umożliwiających stronie zależnej upewnienie się na podstawie certyfikatu:
 - (i) co do tożsamości dostawcy usług certyfikacyjnych;
 - (ii) że podpisujący, który został rozpoznany w certyfikacie ma władzę nad danymi do stworzenia podpisu w momencie, gdy certyfikat został wydany;
 - (iii) dane do stworzenia podpisu były ważne w momencie, gdy certyfikat był wydany lub wcześniej;
- (d) dostarczać dostępnych środków umożliwiających stronie zależnej upewnienie się, gdzie stosowne, na podstawie certyfikatu lub w jakikolwiek inny sposób co do:
 - (i) metody użytej do identyfikacji podpisującego;
 - (ii) istnienia jakiegokolwiek ograniczenia co do celu lub wartości, dla której dane do stworzenia podpisu lub certyfikat mogą być wykorzystane;
 - (iii) faktu, że dane do stworzenia podpisu są ważne i nie zostały przejęte;
 - (iv) istnienia jakiegokolwiek ograniczenia lub rozszerzenia zakresu odpowiedzialności, zastrzeżonego przez dostawcę usług certyfikacyjnych;
 - (v) w przypadku istnienia środków, o których podpisujący ma obowiązek powiadomić na podstawie ustępu 1 punkt (b) artykułu 8 ustawy;
 - (vi) oferty czasowego przywrócenia usług;
- (e) gdy usługi opisane w punkcie (d)(v) zostały zaoferowane, dostarczyć podpisującemu środków, aby dokonał powiadomienia zgodnie z artykułem 8 ustęp 1 punkt (b) ustawy, i, gdy usługi opisane w punkcie (d) (vi) zostały zaoferowane, zapewnić dostępność czasowo przywróconych usług.
- (f) wykorzystywać do świadczenia swoich usług systemów, procedur i zasobów ludzkich godnych zaufania.

2. Dostawca usług certyfikacyjnych ponosi prawne konsekwencje swoich zaniedbań w spełnieniu wymagań opisanych w ustępie 1.

Artykuł 10. Wiarygodność

Dla celów określonych w ustępie 1 punkt (f) artykułu 9 ustawy, aby ustalić, czy lub w jakich granicach, systemy, procedury i zasoby ludzkie wykorzystywane przez dostawcę usług internetowych są wiarygodne, należy mieć na względzie następujące czynniki:

- (a) finansowe i ludzkie zasoby, włączając w to istnienie środków zabezpieczających;
- (b) jakość sprzętu i systemów oprogramowania;
- (c) procedury tworzenia certyfikatów, aplikacji dla certyfikatów i przechowywania danych;
- (d) dostępność informacji dla podpisujących, zidentyfikowanych w certyfikatach i dla potencjalnych osób zależnych;

- (e) systematycznosc i zasieg kontroli niezaleznego podmiotu;
- (f) istnienie deklaracji dokonanej przez Panstwo, podmiotu akredytujacego lub dostawcy uslug certyfikacyjnych dotyczace zgodnosci z lub spelnienia powyzej wymienionych czynnikow; lub
- (g) jakiegokolwiek inne stosowne czynniki.

Artykul 11. Zachowanie stron zaleznych

Strona zalezna ponosi konsekwencje prawne swojego zaniedbania w:

- (a) dokonaniu zasadnych krokow w celu zweryfikowania rzetelnosci podpisu elektronicznego; lub
- (b) dokonaniu zasadnych krokow, gdy podpis elektroniczny jest wsparty certyfikatem, polegajacych na:
 - (i) weryfikacji waznosci, zawieszenia lub przywrócenia waznosci certyfikatu;
 - (ii) stwierdzeniu istnienia jakiegokolwiek ograniczen w odniesieniu do certyfikatu.

Artykul 12. Uznawanie zagranicznych certyfikatow i podpisow elektronicznych

1. Dla swej prawnej skutecznosci podpis elektroniczny lub certyfikat, albo dla ustalenia granic prawnej skutecznosci, podpis elektroniczny lub certyfikat bezwzgleinnie powinien zawierac:
 - (a) polozenie geograficzne, okreslajace gdzie certyfikat zostal wydany albo gdzie podpis elektroniczny zostal stworzony lub wykorzystany;
 - (b) polozenie geograficzne miejsca prowadzenia dzialalnosci gospodarczej przez wydawce albo podpisujacego.
2. Certyfikat wydany poza granicami [Panstwa wydajacego ustawie] ma te sama skutecznosc prawna w [Panstwie wydajacym Ustawie] co certyfikat wydany w [Panstwie wydajacym Ustawie], jesli zapewnia rzeczywista równosc poziomu rzetelnosci.
3. Podpis elektroniczny stworzony lub uzywany poza granicami [Panstwa wydajacego Ustawie] ma te sama skutecznosc prawna co podpis elektroniczny stworzony lub uzywany w [Panstwie wydajacym Ustawie], jesli zapewnia rzeczywista równosc poziomu rzetelnosci;
4. Aby okreslic czy certyfikat albo podpis elektroniczny zapewnia rzeczywista równosc poziomu rzetelnosci dla celow ustepow 2 i 3 tego artykulu nalezy miec na wzgledzie miedzynarodowe standardy i inne odpowiednie czynniki.
5. Gdzie, nie baczac na ustep 2, 3 i 4 tego artykulu, strony umawiaja sie miedzy soba, ze beda uzywac okreslonych typow podpisow elektronicznych lub certyfikatow, umowa ta jest traktowana jako wystarczajaca dla celow uznania ich, chyba ze umowa ta nie bylaby wazna lub skuteczna pod stosowanym prawem.