

## Podpis elektroniczny

Krzysztof Wąs, 30 kwiecień 2009

Do niedawna podstawową formą autoryzowania pisemnej wypowiedzi (w tym oświadczenia woli) był złożony pod jej treścią podpis. Przyjmuje się, że podpisem jest językowy znak graficzny sporządzony własnoręcznie przez oświadczającego, zawierający co najmniej jego nazwisko (zob. *Z. Radwański*, Elektroniczna forma czynności prawnej, Monitor Prawniczy nr 22/2001). Ustawa z dnia 18 września 2001 r. o podpisie elektronicznym (Dz. U. 2001 Nr 130 poz. 1450, dalej: u.p.e.) wprowadziła w tej materii zmiany mające na celu dostosowanie polskiego prawa do coraz szybszego rozwoju informatycznego i norm międzynarodowych, w tym dyrektywy Parlamentu Europejskiego i Rady nr 1999/93 z dnia 13 grudnia 1999 r. w sprawie podpisu elektronicznego oraz ustaw modelowych UNCITRAL (*United Nation Commission on International Trade Law* - komisja ONZ do spraw międzynarodowego prawa handlowego) o handlu elektronicznym z 1999 r. i o podpisach elektronicznych z 2001 r.

Zgodnie z art. 3 ust. 1 u.p.e. podpis elektroniczny to dane w postaci elektronicznej, które wraz z innymi danymi, do których zostały dołączone lub z którymi są logicznie powiązane, służą do identyfikacji osoby składającej podpis elektroniczny.

Doktryna wyróżnia 3 kategorie podpisu elektronicznego (*D. Szostek*, Prawne aspekty podpisu elektronicznego [w:] *J. Barta, R. Markiewicz* (red.) Handel elektroniczny, prawne problemy, Warszawa 2005), a mianowicie:

1. zwykły podpis elektroniczny,
2. bezpieczny podpis elektroniczny oraz
3. bezpieczny podpis elektroniczny weryfikowany przy pomocy kwalifikowanego certyfikatu.

Taka klasyfikacja koresponduje z treścią ustawy o podpisie elektronicznym.

Zwykły podpis elektroniczny to sygnatura dołączona do oświadczenia, która identyfikuje autora wypowiedzi. Sygnatura ta niekoniecznie musi mieć formę nazwiska nadawcy. Zważywszy, że podpis elektroniczny to dane elektroniczne, które są immanentnie związane z wiadomością, to elektroniczną sygnaturę mogą stanowić takie dane jak: adres poczty elektronicznej czy IP (ang. *Internet Protocol* - protokół komunikacyjny używany powszechnie w Internecie i sieciach lokalnych). Zwykły podpis elektroniczny to „podpis”, który nie jest weryfikowany kwalifikowanym certyfikatem. Nie można jednak z tego powodu odmówić mu ważności i skuteczności (zob. art. 8 u.p.e.). Jego moc dowodowa jest równa oświadczeniu złożonemu w formie ustnej (*D. Szostek*, Prawne aspekty podpisu elektronicznego, s. 195). Regułą zawartą art. 8 u.p.e. podkreśla art. 60 k.c., który wyraźnie stanowi, iż oświadczenie woli może zostać złożone w formie elektronicznej. Norma ta nie zastrzega spełnienia żadnych dodatkowych warunków dla skuteczności tak złożonego oświadczenia woli. „Dla rozwoju obrotu

REKLAMA

Potrzebujesz strony internetowej?

olgroup

www.olgroup.pl

www.olgroup.pl

elektronicznego byłoby dobrze, gdyby sądy dopuszczały tego rodzaju dowód jako zaczątek dowodu na piśmie.” (*D. Szostek*, Prawne aspekty podpisu elektronicznego, s. 195).

Natomiast bezpieczny podpis elektroniczny to, w myśl ustawy o podpisie elektronicznym, podpis, który:

- a) jest przyporządkowany wyłącznie do osoby składającej ten podpis,
- b) jest sporządzany za pomocą podlegających wyłącznej kontroli osoby składającej podpis elektroniczny bezpiecznych urządzeń służących do składania podpisu elektronicznego i danych służących do składania podpisu elektronicznego,
- c) jest powiązany z danymi, do których został dołączony, w taki sposób, że jakakolwiek późniejsza zmiana tych danych jest rozpoznawalna (art. 3 pkt 2 u.p.e.).

Jeżeli bezpieczny podpis elektroniczny jest weryfikowany przy pomocy ważnego, kwalifikowanego certyfikatu, jest równoważny podpisowi własnoręcznemu. Oznacza to, że dane w postaci elektronicznej opatrzone bezpiecznym podpisem elektronicznym weryfikowanym przy pomocy ważnego kwalifikowanego certyfikatu są równoważne pod względem skutków prawnych oświadczeniu złożonemu w formie pisemnej (art. 5 ust. 2 u.p.e.). Równoważność formy polega na tym, że skutki przewidziane dla formy pisemnej wystąpią zarówno, gdy składający oświadczenie podpisze je własnoręcznie jak i, jeżeli oświadczenie występuje w formie elektronicznej, opatrzony je bezpiecznym podpisem elektronicznym weryfikowanym przy pomocy ważnego, kwalifikowanego certyfikatu. Reguła równoważności nie obowiązuje, jeżeli istnieje *lex specialis* wyłączający jej stosowanie w określonym zakresie.

By podpis elektroniczny w aspekcie funkcjonalnym był traktowany jak podpis własnoręczny winien spełniać funkcje: gwarantującą, świadczącą, ostrzegawczą oraz identyfikującą (*P. Turek*, Cywilnoprawne skutki podpisu elektronicznego - nie dyskryminować, Edukacja Prawnicza nr 6/2003; por. *W. Kocot*, Charakter prawny podpisu elektronicznego, Przegląd Prawa Handlowego nr 4/2002, *D. Szostek*, Prawne aspekty podpisu elektronicznego, s. 187 i n.). Funkcja gwarantująca to domniemanie prawdziwości złożonego oświadczenia (dokumentu elektronicznego). Funkcja świadcząca potwierdza, iż dokument nie jest projektem, lecz ostatecznym i wyraźnym oświadczeniem woli. Funkcja ostrzegawcza jest spełniona, gdy chroni przed dokonaniem nie do końca przemyślanej czynności prawnej. Funkcja identyfikująca ma na celu wskazanie osoby, która złożyła dane oświadczenie.

R E K L A M A



## e-inkubator

**e-biznes bez ZUS**  
**doradztwo prawne**  
**pożyczki z Funduszu Mikro**

## Znakowanie czasem

Podpis elektroniczny może być znakowany czasem. Stanowi o tym art. 7 ust. 1 u.p.e.. Według ustawowej definicji z art. 3 pkt 16 u.p.e. znakowanie czasem to usługa polegająca na dołączaniu do danych w postaci elektronicznej logicznie powiązanych z danymi opatrzonymi podpisem lub poświadczeniem elektronicznym, oznaczenia czasu w chwili wykonania tej usługi oraz poświadczenia elektronicznego tak powstałych danych przez podmiot świadczący tę usługę.

Znakowanie czasem przez kwalifikowany podmiot świadczący usługi certyfikacyjne wywołuje skutki prawne daty pewnej w rozumieniu przepisów Kodeksu cywilnego. Tak więc czynność prawna opatrzona takim „datownikiem” jest skuteczna względem osób trzecich (*Z. Radwański, op.cit.*; por. *D. Szostek, Czynność prawna a środki komunikacji elektronicznej, Zakamycze 2004, s. 248*). Znakowanie czasem ma na celu potwierdzenie, że dokument istniał w chwili poświadczenia daty (*W. Kocot, op.cit., s. 44*).

Ponadto ustawa zawiera domniemanie, że podpis elektroniczny znakowany czasem przez kwalifikowany podmiot świadczący usługi certyfikacyjne został złożony nie później niż w chwili dokonywania tej usługi. Domniemanie to istnieje do dnia utraty ważności zaświadczenia certyfikacyjnego wykorzystywanego do weryfikacji takiego znakowania. Przedłużenie istnienia domniemanie wymaga kolejnego znakowania czasem podpisu elektronicznego wraz z danymi służącymi do poprzedniej weryfikacji przez kwalifikowany podmiot świadczący tę usługę (art. 7 ust. 3 u.p.e.).

Znakowanie czasem może dotyczyć każdego podpisu elektronicznego, nie tylko tego, który równoważny jest formie pisemnej (bezpieczny podpis weryfikowany przy pomocy ważnego kwalifikowanego certyfikatu) (*D. Szostek, Czynność prawna a środki komunikacji elektronicznej, s. 247*; por. *A. Stosio, Umowy zawierane przez Internet, Warszawa 2002, s. 200*). Co więcej, usługa znakowania czasem może być świadczona przez każdy podmiot. Działalność ta nie wymaga koncesji ani zezwolenia. Jednak, by elektroniczne znakowanie czasem wywołało skutki daty pewnej musi być dokonane przez podmiot kwalifikowany, tj. taki, który został wpisany do rejestru kwalifikowanych podmiotów świadczących usługi certyfikacyjne na mocy decyzji administracyjnej ministra właściwego ds. gospodarki.

Autor jest studentem V roku prawa na Uniwersytecie Śląskim w Katowicach.	Więcej publikacji na <a href="http://www.iprawo.net.pl">www.iprawo.net.pl</a> .
<b>Prawa autorskie</b> Na artykuł udziela się licencji Creative Commons Uznanie autorstwa-Bez utworów zależnych 2.5 Polska <a href="http://creativecommons.org/licenses/by-nd/2.5/pl">http://creativecommons.org/licenses/by-nd/2.5/pl</a>	<b>Wydawca</b> Grupa Interium <a href="http://www.interium.biz">www.interium.biz</a>