

Federalna Ustawa o Podpisie Elektronicznym

(Prawo o podpisie — *SigG*)

Rozdział I *Cel ustawy i definicje*

§ 1 Cel i zakres ustawy

- (1) Niniejsza ustawa federalna wyznacza ramy prawne regulujące tworzenie i używanie podpisów elektronicznych oraz świadczenie usług związanych z podpisami i certyfikatami.
- (2) Niniejsza ustawa federalna stosuje się do systemów zamkniętych, w zakresie uzgodnionym przez użytkowników danego systemu w drodze umownej, a także do otwartych transakcji elektronicznych przeprowadzanych z sądami i innymi władzami, z wyłączeniem przypadków uregulowanych inaczej przez prawo.

§ 2 Definicje

Dla celów niniejszej ustawy federalnej obowiązują poniższe definicje.

1. **Podpis elektroniczny:** dane elektroniczne dołączone do innych danych elektronicznych lub z nimi logicznie powiązane, służące do uwierzytelnienia, czyli do potwierdzenia tożsamości sygnatariusza.
2. **Sygnatariusz:** osoba fizyczna, której zostały przydzielone dane do tworzenia podpisu i odpowiadające im dane do weryfikacji podpisu, a która tworzy podpis elektroniczny we własnym imieniu lub w imieniu osoby trzeciej, a także usługodawca certyfikacyjny, który używa certyfikatów do świadczenia usług certyfikacyjnych.

3. **Bezpieczny podpis elektroniczny:** podpis elektroniczny, który spełnia następujące warunki:
 - a) jest przydzielony wyłącznie sygnatariuszowi;
 - b) umożliwia ustalenie tożsamości sygnatariusza;
 - c) jest utworzony przy użyciu urządzeń, które znajdują się pod wyłączną kontrolą sygnatariusza;
 - d) jest powiązany z opatrzonymi tym podpisem danymi w sposób umożliwiający stwierdzenie, czy nastąpiła jakakolwiek zmiana w danych po złożeniu podpisu;
 - e) jest oparty na kwalifikowanym certyfikacie oraz jest utworzony przy użyciu środków technicznych i procedur zgodnych z wymaganiami w zakresie zabezpieczeń, stawianymi przez niniejszą ustawę federalną i przez rozporządzenia wydane na jej podstawie.

4. **Dane do tworzenia podpisu:** niepowtarzalne dane, takie jak kody lub prywatne klucze kodowe, którymi posługuje się sygnatariusz przy tworzeniu podpisu elektronicznego.

5. **Urządzenie do tworzenia podpisu:** konfiguracja oprogramowania i sprzętu umożliwiająca uzyskanie danych do tworzenia podpisu.

6. **Dane do weryfikacji podpisu:** dane, takie jak kody lub publiczne klucze kodowe, które służą do weryfikacji podpisu elektronicznego.

7. **Urządzenie do weryfikacji podpisu:** konfiguracja oprogramowania i sprzętu używana do przetwarzania danych do weryfikacji podpisu.

8. **Certyfikat:** informacja elektroniczna wiążąca dane do weryfikacji podpisu z określoną osobą, której tożsamość jest określona przez certyfikat.

9. **Certyfikat kwalifikowany:** certyfikat zawierający informacje, o których mowa w § 5, wydany przez usługodawcę certyfikacyjnego spełniającego wymagania określone w § 7.

10. **Usługodawca certyfikacyjny:** osoba fizyczna lub prawna, względnie inny podmiot zdolny do czynności prawnych, która (który) wydaje certyfikaty lub świadczy inne usługi związane z podpisami i certyfikatami.
11. **Usługi związane z podpisami i certyfikatami:** dostarczanie produktów sygnaturowych i udostępnianie procedur składania podpisów elektronicznych, wydawanie i odnawianie certyfikatów, administrowanie certyfikatami, a także świadczenie usług katalogowania, unieważniania, rejestracji, opatrywania datownikiem, komputerowego przetwarzania oraz udzielania porad w związku z podpisami elektronicznymi.
12. **Datownik:** potwierdzenie wydane przez usługodawcę certyfikacyjnego i opatrzone przezeń podpisem elektronicznym, zaświadczające fakt przedłożenia określonych danych elektronicznych w określonym czasie.
13. **Produkt sygnaturowy:** sprzęt, oprogramowanie lub określone składniki sprzętowe czy programowe, służące do tworzenia i weryfikacji podpisów elektronicznych lub używane przez usługodawcę certyfikacyjnego do świadczenia usług związanych z podpisami i certyfikatami.
14. **Naruszenie:** złamanie środków lub technik zabezpieczeń, w wyniku którego przestaje mieć zastosowanie poziom zabezpieczenia ustalony przez usługodawcę certyfikacyjnego.

Rozdział 2

Zakres stosowania ustawy o podpisie elektronicznym

§ 3

Ogólne skutki prawne

- (1) Przy przeprowadzaniu transakcji prawnych i handlowych mogą być stosowane procedury składania podpisów elektronicznych o różnych poziomach zabezpieczenia i różnych klasach certyfikatów.

- (2) W konsekwencji ust. (1) nie można wyłączyć skutków prawnych podpisu elektronicznego i jego dopuszczalności jako dowodu jedynie z tego powodu, że podpis elektroniczny występuje tylko w formie elektronicznej, że nie jest oparty na kwalifikowanym certyfikacie, że nie jest oparty na kwalifikowanym certyfikacie wydanym przez akredytowanego usługodawcę certyfikacyjnego, bądź że nie został utworzony przy użyciu środków technicznych i procedur określonych w § 18.

§ 4 **Szczegółowe skutki prawne**

- (1) Bezpieczny podpis elektroniczny spełnia wymogi prawne stawiane wobec podpisu ręcznego, a w szczególności wymogi dotyczące formy pisemnej, określonej w § 886 Austriackiego Kodeksu Cywilnego, chyba że prawo lub umowa między stronami reguluje to inaczej.
- (2) Bezpieczny podpis elektroniczny nie ma skutków prawnych formy pisemnej, określonej w § 886 Austriackiego Kodeksu Cywilnego, w następujących przypadkach:
1. przy czynnościach prawnych przewidzianych przez prawo rodzinne i prawo spadkowe, dla których wymagana jest forma pisemna lub wobec których stawiane są ściślejsze wymagania formalne;
 2. przy innych oświadczeniach woli i czynnościach prawnych, których ważność jest uwarunkowana potwierdzeniem oficjalnym, poświadczeniem sądowym lub notarialnym bądź zachowaniem formy aktu notarialnego;
 3. przy oświadczeniach woli, czynnościach prawnych i wnioskach, których wprowadzenie do księgi wieczystej, rejestru handlowego lub innego rejestru jest uwarunkowane potwierdzeniem oficjalnym, poświadczeniem sądowym lub notarialnym bądź zachowaniem formy aktu notarialnego;
 4. przy deklaracjach gwarancji, o których mowa w § 1346 ust. 2 Austriackiego Kodeksu Cywilnego.
- (3) Postanowienia § 294 Kodeksu Postępowania Cywilnego, regulujące domniemanie autentyczności treści podpisanego dokumentu prywatnego, rozciągają się także na dokumenty elektroniczne opatrzone bezpiecznym podpisem elektronicznym.

- (4) Skutki prawne określone w ust. (1) i (3) nie występują w przypadku, gdy zostanie udowodnione, że wymagania w zakresie zabezpieczeń stawiane przez niniejszą ustawę federalną i przez rozporządzenia wydane na jej podstawie nie zostały spełnione, bądź też że nastąpiło naruszenie środków podjętych w celu spełnienia wspomnianych wyżej wymagań.

§ 5 **Certyfikaty kwalifikowane**

- (1) Certyfikat kwalifikowany musi zawierać co najmniej następujące informacje:
1. oznaczenie, że certyfikat ten jest certyfikatem kwalifikowanym;
 2. nazwa usługodawcy certyfikacyjnego i kraju, w którym został on ustanowiony, określone w formie wykluczającej pomyłkę;
 3. imię i nazwisko sygnatariusza bądź pseudonim sygnatariusza wraz z oznaczeniem, że jest to pseudonim;
 4. informacja na temat pełnomocnictw lub innych ważnych atrybutów prawnych sygnatariusza (jeżeli wnioskodawca tego zażąda);
 5. dane do weryfikacji podpisu, przydzielone sygnatariuszowi;
 6. data początkowa i końcowa okresu ważności certyfikatu;
 7. niepowtarzalny identyfikator certyfikatu;
 8. ograniczenie zakresu certyfikatu, o ile takie występuje;
 9. ograniczenie wartości transakcji zawieranych przy użyciu certyfikatu, o ile takie występuje.
- (2) Na żądanie wnioskodawcy w certyfikacie kwalifikowanym mogą zostać zamieszczone inne ważne informacje prawne.
- (3) Certyfikat kwalifikowany musi być opatrzony bezpiecznym podpisem elektronicznym usługodawcy certyfikacyjnego.

Rozdział 3

Usługodawcy certyfikacyjni

§ 6

Działalność usługodawców certyfikacyjnych

- (1) Usługodawca certyfikacyjny nie musi uzyskiwać żadnego specjalnego zezwolenia na rozpoczęcie i prowadzenie działalności.
- (2) Każdy usługodawca certyfikacyjny jest zobowiązany niezwłocznie powiadomić organ nadzorczy, o którym mowa w § 13, o rozpoczęciu swojej działalności. Przed rozpoczęciem działalności lub zmianą świadczonych przez siebie usług usługodawca certyfikacyjny jest zobowiązany złożyć we wspomnianym organie nadzorczym reguły zabezpieczenia i certyfikacji dla każdej świadczonej przez siebie usługi związanej z podpisami i certyfikatami.
- (3) Reguły zabezpieczenia składane przez usługodawcę certyfikacyjnego, który dostarcza procedury składania zabezpieczonych podpisów elektronicznych, muszą opisywać, w jaki sposób procedury te zapewniają zgodność z wymaganiami w zakresie zabezpieczeń stawianymi przez niniejszą ustawę federalną i przez rozporządzenia wydane na jej podstawie.
- (4) Usługodawca certyfikacyjny jest zobowiązany przestrzegać zgłoszonych przez siebie reguł zabezpieczenia i certyfikacji, zarówno przy rozpoczynaniu działalności, jak i przez cały okres jej prowadzenia.
- (5) Usługodawca certyfikacyjny jest zobowiązany niezwłocznie powiadomić organ nadzorczy o każdej okoliczności, która uniemożliwia niezakłócone prowadzenie działalności zgodnie z regułami zabezpieczenia i certyfikacji.
- (6) Reguły zabezpieczenia składane przez usługodawcę certyfikacyjnego, który wydaje certyfikaty, muszą określać, czy świadczone są także usługi katalogowania i unieważniania, a jeżeli tak, to w jakiej formie są one świadczone.

- (7) Usługodawca certyfikacyjny może używać swojego certyfikatu tylko do świadczenia usług certyfikacyjnych.

§ 7

Usługodawcy certyfikacyjni wydający certyfikaty kwalifikowane

- (1) Usługodawca certyfikacyjny wydający certyfikaty kwalifikowane musi spełniać następujące warunki:
1. wykazać, że zapewnia niezawodność wymaganą do świadczenia usług związanych z podpisami i certyfikatami;
 2. świadczyć szybkie i zabezpieczone usługi katalogowania oraz natychmiastowe i zabezpieczone usługi unieważniania;
 3. przy wydawaniu certyfikatów kwalifikowanych oraz świadczeniu usług katalogowania i unieważniania stosować dane określające czas (datownik) o gwarantowanej dokładności, a także zapewnić zawsze możliwość ustalenia czasu wydania lub unieważnienia certyfikatu kwalifikowanego;
 4. sprawdzać w sposób wiarygodny — na podstawie oficjalnych dokumentów tożsamości ze zdjęciem — tożsamość i ewentualnie inne ważne atrybuty prawne osoby, której zostaje wydany certyfikat kwalifikowany;
 5. zatrudniać rzetelnych pracowników dysponujących specjalistyczną wiedzą, doświadczeniem i kwalifikacjami, a w szczególności umiejętnościami i wiedzą w zakresie technologii bezpiecznych podpisów i odpowiednich procedur zabezpieczeń wymaganych dla świadczenia usług, a także stosować odpowiednie procedury administracji i zarządzania, zgodnie z uznanymi standardami;
 6. dysponować dostatecznymi środkami finansowymi do tego, by spełnić wymagania stawiane przez niniejszą ustawę federalną i przez rozporządzenia wydane na jej podstawie, a także podjąć odpowiednie działania na wypadek roszczeń o odszkodowanie, na przykład polegające na zawarciu ubezpieczenia od odpowiedzialności cywilnej;
 7. rejestrować wszystkie istotne fakty odnoszące się do certyfikatów kwalifikowanych i przechowywać je przez czas odpowiedni do ich charakteru, w tym w razie potrzeby w formie elektronicznej, tak aby można było

udowodnić fakt certyfikacji, w szczególności w trakcie postępowania sądowego;

8. podjąć odpowiednie środki ostrożności, uniemożliwiające przechowywanie lub kopiowanie danych do tworzenia podpisów poszczególnych sygnatariuszy, zarówno przez usługodawcę certyfikacyjnego, jak i przez osoby trzecie.
- (2) Usługodawca certyfikacyjny wydający certyfikaty kwalifikowane musi stosować niezawodne systemy, produkty i procedury, które zapewniają ochronę przed modyfikacją oraz zapewniają techniczne i kryptograficzne zabezpieczenie usług związanych z podpisami i certyfikatami odnoszących się do tworzenia i przechowywania certyfikatów. Usługodawca certyfikacyjny musi przede wszystkim podjąć odpowiednie środki ostrożności gwarantujące utrzymanie w tajemnicy danych do tworzenia podpisu, tak aby dane do certyfikatów kwalifikowanych nie mogły zostać podrobione lub sfalszowane w sposób niezauważony, a także aby certyfikaty były udostępniane publicznie przez sieć informatyczną tylko za zgodą sygnatariusza. Przy dostarczaniu danych do tworzenia podpisów oraz przy tworzeniu i przechowywaniu certyfikatów kwalifikowanych usługodawca certyfikacyjny musi stosować środki techniczne i procedury zgodne z wymaganiami podanymi w § 18.
 - (3) Dane do tworzenia podpisu usługodawcy certyfikacyjnego muszą być zabezpieczone przed dostępem osób nieupoważnionych.
 - (4) Fakt spełnienia warunków określonych przez ust. (1), (2) i (3) w odniesieniu do bezpiecznych podpisów elektronicznych może być poświadczany w trakcie procedury dobrowolnej akredytacji, o której mowa w § 17.
 - (5) Jeżeli usługodawca certyfikacyjny udostępnia procedurę składania bezpiecznego podpisu elektronicznego, to fakt, że jest to bezpieczny podpis elektroniczny, musi być zaznaczony w certyfikacie lub w katalogu dostępnym powszechnie i bez przerwy przez sieć informatyczną.

- (6) Na żądanie sądu lub innych władz usługodawca certyfikacyjny będzie zobowiązany zweryfikować bezpieczny podpis oparty na certyfikacie kwalifikowanym wydanym przez tego usługodawcę.

§ 8

Wydawanie certyfikatów kwalifikowanych

- (1) Usługodawca certyfikacyjny jest zobowiązany ustalić w sposób wiarygodny — na podstawie oficjalnych dokumentów tożsamości ze zdjęciem — tożsamość osoby, której zostaje wydany certyfikat kwalifikowany. Przez wydanie certyfikatu kwalifikowanego usługodawca certyfikacyjny potwierdza, że takiej osobie zostały przydzielone określone dane do certyfikacji podpisu.
- (2) Wniosek o wydanie certyfikatu kwalifikowanego może być także złożony do organu wskazanego przez usługodawcę certyfikacyjnego. Organ taki sprawdza tożsamość wnioskodawcy.
- (3) Na żądanie wnioskodawcy usługodawca certyfikacyjny ma obowiązek zamieścić w certyfikacie kwalifikowanym informacje dotyczące pełnomocnictw wnioskodawcy i innych jego ważnych atrybutów prawnych, zgodnie z deklaracją zasad certyfikacji, pod warunkiem że potwierdzane w ten sposób fakty zostaną w sposób wiarygodny udowodnione wobec usługodawcy certyfikacyjnego lub wobec organu, o którym mowa w ust. (2).
- (4) Na żądanie wnioskodawcy usługodawca certyfikacyjny może zamieścić zamiast imienia i nazwiska sygnatariusza jego pseudonim, zgodnie z deklaracją zasad certyfikacji. Pseudonim nie może mieć charakteru obraźliwego ani formy stwarzającej możliwość jego pomylenia z nazwiskami czy innymi znakami.

§ 9

Unieważnianie certyfikatów

- (1) Usługodawca certyfikacyjny jest zobowiązany niezwłocznie unieważnić certyfikat w każdym z następujących przypadków:
1. kiedy zażąda tego sygnatariusz lub przełożony wskazany w certyfikacie;

2. kiedy usługodawca certyfikacyjny uzyska informację o śmierci sygnatariusza lub o jakiegokolwiek zmianie faktów potwierdzonych w certyfikacie;
 3. kiedy okaże się, że certyfikat został uzyskany na podstawie fałszywych informacji;
 4. kiedy usługodawca certyfikacyjny zaprzestanie działalności, a usługi katalogowania i unieważniania nie zostaną przejęte przez innego usługodawcę certyfikacyjnego;
 5. kiedy organ nadzorczy nakaże unieważnienie certyfikatu zgodnie z § 14;
 6. kiedy zachodzi obawa, że certyfikat zostanie wykorzystany w sposób niewłaściwy.
- (2) Jeżeli okoliczności, o których mowa w ust. (1), nie mogą być natychmiast stwierdzone poza wszelką wątpliwość, usługodawca certyfikacyjny jest zobowiązany niezwłocznie zablokować certyfikat.
- (3) Zablokowanie lub unieważnienie certyfikatu musi zawierać datę i godzinę wejścia w życie. Jeżeli usługodawca certyfikacyjny świadczy usługi unieważniania, zablokowanie lub unieważnienie certyfikatu obowiązuje od momentu wprowadzenia zmiany do odpowiedniego katalogu. Nie jest dopuszczalne zablokowanie lub unieważnienie certyfikatu z mocą wsteczną. Sygnatariusz lub jego następcą prawny musi zostać niezwłocznie powiadomiony o zablokowaniu lub unieważnieniu certyfikatu.
- (4) Usługodawca certyfikacyjny jest zobowiązany udostępniać wykaz zablokowanych i unieważnionych certyfikatów kwalifikowanych. Wykaz ten musi być uwidoczniony bez przerwy w powszechnie dostępnej sieci informatycznej.
- (5) Organ nadzorczy jest zobowiązany niezwłocznie unieważnić certyfikat usługodawcy certyfikacyjnego w każdym z następujących przypadków:
1. kiedy usługodawcy certyfikacyjnemu zostanie zakazane prowadzenie działalności, a jego usługi katalogowania i unieważniania nie zostaną przejęte przez innego usługodawcę certyfikacyjnego;

2. kiedy usługodawca certyfikacyjny zawiesi działalność, a jego usługi katalogowania i unieważniania nie zostaną przejęte przez innego usługodawcę certyfikacyjnego.

§ 10 **Usługi opatrywania datownikiem**

Jeżeli usługodawca certyfikacyjny świadczy usługi opatrywania datownikiem, musi to szczegółowo udokumentować w deklaracji reguł zabezpieczenia i certyfikacji. Przy świadczeniu usług opatrywania datownikiem usługodawca certyfikacyjny musi stosować środki techniczne i procedury zapewniające poprawność i autentyczność oznaczenia czasu, zgodnie z wymaganiami podanymi w § 18.

§ 11 **Rejestry**

- (1) Usługodawca certyfikacyjny jest zobowiązany rejestrować środki zabezpieczenia podejmowane w celu zapewniania zgodności z wymaganiami stawianymi przez niniejszą ustawę federalną i przez rozporządzenia wydane na jej podstawie, a także rejestrować fakty wydania, zablokowania i unieważnienia certyfikatów. Musi być zawsze zapewniona możliwość weryfikacji tych danych, ich autentyczności oraz daty wprowadzenia do rejestru.
- (2) Usługodawca certyfikacyjny jest zobowiązany na żądanie sądu lub innych władz przedstawiać rejestry, o których mowa w ust. (1).

§ 12 **Zawieszenie działalności**

Usługodawca certyfikacyjny jest zobowiązany niezwłocznie powiadomić organ nadzorczy o zawieszeniu działalności. W przypadku zawieszeniu działalności usługodawca certyfikacyjny jest także zobowiązany unieważnić wszystkie ważne certyfikaty albo zapewnić przejęcie przez innego usługodawcę certyfikacyjnego przynajmniej usług katalogowania i unieważniania. Każdy sygnatariusz musi być niezwłocznie powiadomiony o zawieszeniu działalności i unieważnieniu certyfikatu lub przejęciu usług. Usługodawca certyfikacyjny jest

zobowiązany zapewnić kontynuowanie usług unieważniania nawet po unieważnieniu certyfikatów. Jeżeli usługodawca certyfikacyjny nie spełni tego obowiązku, organ nadzorczy spowoduje kontynuowanie usług unieważniania na koszt tego usługodawcy certyfikacyjnego.

Rozdział 4 Nadzór

§ 13 Organ nadzorczy

- (1) Jako organ nadzorczy będzie działać Komisja Kontroli Telekomunikacji (*Telekom-Control-Kommission*), ustanowiona na mocy § 110 ustawy „Prawo telekomunikacyjne”. Organ nadzorczy będzie odpowiedzialny za stały nadzór nad przestrzeganiem postanowień niniejszej ustawy federalnej i rozporządzeń wydanych na jej podstawie.
- (2) Organ nadzorczy będzie w szczególności wykonywać następujące czynności:
 1. kontrolować, czy reguły zabezpieczenia i certyfikacji zawarte w deklaracji są faktycznie realizowane;
 2. monitorować, czy usługodawcy certyfikacyjni dostarczający bezpieczne podpisy elektroniczne stosują odpowiednie środki techniczne i procedury, o których mowa w § 18;
 3. dokonywać akredytacji usługodawców certyfikacyjnych zgodnie z § 17 i § 4 *[w § 4 nie ma mowy o akredytacji – przyp. BTInfo]* oraz nadzorować organizację instytucji zatwierdzających, o których mowa w § 19;
- (3) Organ nadzorczy zapewni powszechną i nieprzerwaną dostępność przez sieć informatyczną katalogu ważnych, zablokowanych i unieważnionych certyfikatów wszystkich usługodawców certyfikacyjnych. Ponadto organ nadzorczy zapewni powszechną i nieprzerwaną dostępność przez sieć informatyczną katalogu usługodawców certyfikacyjnych zgłoszonych w Austrii, katalogu usługodawców certyfikacyjnych akredytowanych przez organ nadzorczy oraz katalogu zagranicznych usługodawców certyfikacyjnych, których certyfikaty są gwarantowane przez usługodawców certyfikacyjnych zgłoszonych w Austrii, zgodnie z postanowieniami §

24 ust. (2) punkt 2. W katalogu tym zostaną także na żądanie umieszczeni inni zagraniczni usługodawcy certyfikacyjni. Katalog certyfikatów usługodawców certyfikacyjnych będzie zawierać certyfikaty kwalifikowane upoważniające tych usługodawców certyfikacyjnych do świadczenia usług certyfikacyjnych. Organ nadzorczy może także wydawać takie certyfikaty. Każdy katalog utrzymywany przez organ nadzorczy zostanie opatrzony bezpiecznym podpisem elektronicznym tego organu. Certyfikat organu nadzorczego zostanie opublikowany w Dzienniku Urzędowym wydawanym przez *Wiener Zeitung*.

- (4) Koszty działalności organu nadzorczego i prac wykonywanych przez spółkę Telekom-Control GmbH będą pokrywane z opłat pobieranych od usługodawców certyfikacyjnych, zgodnie z odnośnym rozporządzeniem. Opłaty te będą pobierane przez organ nadzorczy, który będzie płacić spółce Telekom-Control GmbH lub instytucji zatwierdzającej za wykonywane przez nie prace.
- (5) Organ nadzorczy może zasięgać porad odpowiednich osób lub instytucji, takich jak instytucje zatwierdzające, o których mowa w § 19.
- (6) Zgodnie z artykułem 20 ust. (2) Konstytucji Federalnej, członkowie organu nadzorczego nie są przy wykonywaniu swych funkcji związani żadnymi instrukcjami. Organ nadzorczy będzie stosować *1991 AVG*, chyba że ustawa stanowi inaczej. Organ nadzorczy jest ostatnią instancją decyzyjną i może się odwoływać do sądów administracyjnych.
- (7) Działalność organu nadzorczego przewidziana w niniejszej ustawie federalnej będzie oddzielona pod względem organizacyjnym i finansowym od działalności tego organu przewidzianej przez inne ustawy federalne.

§ 14 **Środki nadzoru**

- (1) Organ nadzorczy zastosuje wobec usługodawców certyfikacyjnych środki nadzorcze zapewniające wypełnianie ich obowiązków nałożonych przez niniejszą ustawę federalną i przez rozporządzenia wydane na jej podstawie. W szczególności organ

nadzorczy może zabronić usługodawcy certyfikacyjnemu stosowania nieodpowiednich środków technicznych i procedur przy świadczeniu niektórych lub wszystkich usług. Ponadto organ nadzorczy może unieważnić certyfikat usługodawcy certyfikacyjnego lub certyfikat sygnatariusza oraz może nakazać usługodawcy certyfikacyjnemu unieważnienie certyfikatu sygnatariusza.

- (2) Z wyjątkiem sytuacji, gdy nakazane zostaną środki naprawcze, o których mowa w ust. (6), prowadzenie działalności usługodawcy certyfikacyjnego zostanie zakazane w całości lub w części, jeśli usługodawca certyfikacyjny dopuści się jakiegokolwiek z poniższych uchybień:
1. usługodawca certyfikacyjny lub jego pracownicy nie wykazują rzetelności niezbędnej przy świadczeniu usług związanych z podpisami i certyfikatami;
 2. usługodawca certyfikacyjny lub jego pracownicy nie posiadają niezbędnej wiedzy specjalistycznej;
 3. usługodawca certyfikacyjny nie dysponuje dostatecznymi zasobami finansowymi;
 4. usługodawca certyfikacyjny nie realizuje w praktyce, w trakcie prowadzenia działalności, reguł zabezpieczenia i certyfikacji określonych w jego deklaracji;
 5. usługodawca certyfikacyjny nie świadczy nakazanych usług katalogowania i unieważniania lub świadczy je nienależycie, bądź nie wypełnia obowiązków blokowania lub unieważniania, o których mowa w § 9, lub wypełnia je nienależycie;
 6. usługodawca certyfikacyjny nie wypełnia obowiązków powiadamiania, o których mowa w § 6 ust. (2).
- (3) Z wyjątkiem sytuacji, gdy nakazane zostaną środki naprawcze, o których mowa w ust. (6), prowadzenie działalności usługodawcy certyfikacyjnego wydającego certyfikaty kwalifikowane zostanie zakazane w całości lub w części, jeżeli nie są spełnione inne warunki regulujące prowadzenie takiej działalności, przewidziane przez niniejszą ustawę federalną i przez rozporządzenia wydane na jej podstawie.
- (4) Z wyjątkiem sytuacji, gdy nakazane zostaną środki naprawcze, o których mowa w ust. (6), prowadzenie działalności usługodawcy certyfikacyjnego udostępniającego

procedury składania bezpiecznych podpisów elektronicznych zostanie zakazane w całości lub w części, jeżeli stosowane przy tym środki techniczne i procedury nie spełniają wymagań w zakresie zabezpieczenia, o których mowa w § 18.

- (5) Jeżeli organ nadzorczy zakaze usługodawcy certyfikacyjnemu prowadzenia działalności, spowoduje także, aby certyfikat usługodawcy certyfikacyjnego i certyfikaty sygnatariuszy zostały unieważnione, bądź spowoduje, aby usługi związane z podpisami i certyfikatami — przynajmniej w części dotyczącej katalogowania i unieważniania — zostały przejęte przez innego usługodawcę certyfikacyjnego. Przejęcie usług, o którym mowa w poprzednim zdaniu, musi się odbyć za zgodą obu usługodawców certyfikacyjnych. Sygnatariusze muszą być niezwłocznie powiadomieni o zakazaniu usługodawcy certyfikacyjnemu prowadzenia działalności i o unieważnieniu certyfikatów lub przejęciu usług. Usługodawca certyfikacyjny jest zobowiązany zapewnić kontynuowanie usług unieważniania nawet po unieważnieniu certyfikatów. Jeżeli usługodawca certyfikacyjny nie spełni tego obowiązku, organ nadzorczy spowoduje kontynuowanie usług unieważniania na koszt tego usługodawcy certyfikacyjnego.
- (6) Organ nadzorczy wstrzyma decyzję zakazującą działalności usługodawcy certyfikacyjnego, jeśli możliwe jest nakazanie środków naprawczych, które w dostatecznym stopniu zagwarantują przestrzeganie postanowień przewidzianych przez niniejszą ustawę federalną i przez rozporządzenia wydane na jej podstawie. W szczególności organ nadzorczy może nałożyć pewne warunki lub zagrozić podjęciem pewnych działań, jeśli uchybienia wskazane przez organ nadzorczy nie zostaną naprawione we wskazanym przezeń, możliwym do przyjęcia terminie.

§ 15

Udział spółki Telekom-Control GmbH

- (1) Organ nadzorczy może przy realizacji swych czynności nadzorczych korzystać z usług spółki Telekom-Control GmbH, o której mowa w § 108 ustawy „Prawo telekomunikacyjne”.
- (2) Spółka Telekom-Control GmbH może wykonywać między innymi następujące usługi:

1. wspomagać organ nadzorczy w codziennym nadzorowaniu usługodawców certyfikacyjnych oraz kontroli produktów technicznych, procedur i innych środków używanych w celu świadczenia usług związanych z podpisami i certyfikatami, a także w kontroli kwalifikacji pracowników;
 2. rejestrować usługodawców certyfikacyjnych, którzy składają zawiadomienie o rozpoczęciu działalności;
 3. utrzymywać katalog certyfikatów usługodawców certyfikacyjnych, katalog certyfikatów innych usługodawców certyfikacyjnych, o których mowa w § 13 ust. (3), oraz katalog akredytowanych usługodawców certyfikacyjnych, o którym mowa w § 17 ust. (1);
 4. kontynuować usługi unieważniania po usługodawcy certyfikacyjnym, którego działalność została zawieszona lub zakazana, jeśli usługi te nie zostały przejęte przez innego usługodawcę zgodnie z § 12 lub § 14 ust. (5);
 5. na żądanie organu nadzorczego badać zgodność z warunkami dobrowolnej akredytacji, o której mowa w § 17;
 6. pomagać w ustaleniu równoważności zagranicznych raportów testowych, o których mowa w § 24 ust. (3);
 7. w przypadku uzasadnionego podejrzenia nieprzestrzegania wymagań w zakresie zabezpieczeń, nałożonych przez niniejszą ustawę federalną i przez rozporządzenia wydane na jej podstawie, a także na żądanie usługodawcy certyfikacyjnego, wprowadzić bezpośrednio czasowy zakaz działalności usługodawcy certyfikacyjnego lub wprowadzić środki nadzorcze, o których mowa w § 14 ust. (1).
- (3) Spółka Telekom-Control GmbH podejmie wszelkie środki organizacyjne niezbędne do zapewnienia jej zdolności do wypełniania obowiązków i wspomagania organu nadzorczego w wypełnianiu jego obowiązków. Spółka Telekom-Control GmbH może korzystać z porad odpowiednich osób lub instytucji, takich jak instytucje zatwierdzające, o których mowa w § 19. Pracownicy spółki Telekom-Control GmbH będą zobowiązani wypełniać polecenia dyrektora lub członka zarządu, mianowanego zgodnie ze statutem spółki jako odpowiedzialnego za współpracę z organem nadzorczym.

- (4) Niezależnie od przysługującego zainteresowanym stronom prawa do wnoszenia spraw do sądu powszechnego, klienci lub inne zainteresowane strony mogą wnosić do spółki Telekom-Control GmbH roszczenia i skargi przeciw usługodawcy certyfikacyjnemu w sprawach, dla których nie zdołano znaleźć zadowalającego rozwiązania bezpośrednio z nim. W szczególności dotyczy to spraw związanych z jakością usług certyfikacyjnych. Spółka Telekom-Control GmbH dołoży wszelkich starań, aby w możliwym do przyjęcia terminie znaleźć rozwiązanie, które zadowoli obie strony. Usługodawca certyfikacyjny jest zobowiązany uczestniczyć w takiej procedurze i dostarczyć wszelkich informacji niezbędnych do oceny sytuacji. Spółka Telekom-Control GmbH ustali wytyczne do realizacji powyższej procedury i opublikuje te wytyczne w odpowiedniej formie.
- (5) § 13 ust. (7), regulujący oddzielenie pod względem organizacyjnym i finansowym, odnosi się także do działalności spółki Telekom-Control GmbH w zakresie wykonywania nadzoru.

§ 16 Wykonywanie nadzoru

- (1) Usługodawca certyfikacyjny jest zobowiązany zapewnić osobom występującym w imieniu organu nadzorczego dostęp do pomieszczeń i obiektów biurowych i operacyjnych w godzinach pracy, przedłożyć lub udostępnić do kontroli księgi oraz inne rejestry i dokumenty, w tym rejestry, o których mowa w § 11, a także udzielić wszelkich innych wymaganych informacji i pomocy. Istniejące gwarancje ustawowe dotyczące zachowania tajemnicy i prawa do nieujawniania pozostają przy tym w mocy.
- (2) Jeżeli zażąda tego organ nadzorczy i osoby występujące w jego imieniu, pomocy przy wykonywaniu nadzoru udziela funkcjonariusze Służby Bezpieczeństwa, działając w granicach swych ustawowych kompetencji.
- (3) Wykonywanie nadzoru, o którym mowa w ust. (1) i (2), będzie sprawowane w taki sposób, aby wywołać jak najmniejsze utrudnienia dla zainteresowanych stron, a także

uniknąć niepotrzebnego przyciągania uwagi, a przy tym zapewnić pełne bezpieczeństwo usług związanych z podpisami i certyfikatami.

§ 17 **Dobrowolna akredytacja**

- (1) Usługodawca certyfikacyjny, który udostępnia procedury składania bezpiecznych podpisów elektronicznych i który udowodni wobec organu nadzorczego przed rozpoczęciem swej działalności jako akredytowanego usługodawcy certyfikacyjnego, że spełnia wymagania nałożone przez niniejszą ustawę federalną i przez rozporządzenia wydane na jej podstawie, zostanie na własne żądanie akredytowany przez organ nadzorczy. Akredytowany usługodawca certyfikacyjny może określać się jako taki za zgodą organu nadzorczego. Usługodawca certyfikacyjny może się określać jako akredytowany usługodawca certyfikacyjny tylko w odniesieniu do usług związanych z podpisami i certyfikatami oraz produktów sygnaturowych, które spełniają wymagania w zakresie zabezpieczenia określone w § 18. Organ nadzorczy spowoduje, że akredytowani usługodawcy certyfikacyjni będą zamieszczeni w katalogu dostępnym powszechnie i bez przerwy przez sieć informatyczną.
- (2) Fakt dobrowolnej akredytacji usługodawcy certyfikacyjnego zostanie zaznaczony w certyfikacie kwalifikowanym lub podany do wiadomości w innej odpowiedniej formie.
- (3) Organ nadzorczy spowoduje, że akredytowani usługodawcy certyfikacyjni będą podlegać regularnemu monitorowaniu.

Rozdział 5 **Wymagania w zakresie zabezpieczenia technicznego**

§ 18 **Środki techniczne i procedury do zapewniania bezpiecznych podpisów elektronicznych**

- (1) Przy generowaniu i przechowywaniu danych do tworzenia podpisu oraz przy tworzeniu bezpiecznych podpisów muszą być stosowane środki techniczne, które

umożliwiają niezawodne wykrycie sfałszowania danych opatrzonych podpisem elektronicznym oraz niezawodnie zapobiegają nieupoważnionemu użyciu procedur składania podpisów i danych do tworzenia podpisu.

- (2) Środki techniczne i procedury stosowane do tworzenia bezpiecznego podpisu muszą także uniemożliwić zmianę danych opatrzonych podpisem. Ponadto te środki techniczne i procedury muszą zapewnić, by dane, które mają zostać podpisane, zostały uwidocznione sygnatariuszowi przed uruchomieniem procedury złożenia podpisu. Prawdopodobieństwo niepowtarzalności danych do tworzenia podpisu musi być bliskie pewności. Dane do tworzenia podpisu muszą być należycie zabezpieczone przed kryptoanalizą oraz musi być zagwarantowane utrzymanie ich w tajemnicy.
- (3) Do tworzenia i przechowywania certyfikatów kwalifikowanych muszą być stosowane środki techniczne i procedury, które zapobiegają sfałszowaniu (podrobieniu lub przerobieniu) certyfikatów.
- (4) Do weryfikacji danych opatrzonych bezpiecznym podpisem muszą być stosowane środki techniczne i procedury, które zapewniają spełnienie następujących warunków:
 1. aby dane opatrzone podpisem nie mogły zostać zmienione;
 2. aby podpis można było niezawodnie zweryfikować, a wyniki weryfikacji prawidłowo uwidocznić;
 3. aby osoba dokonująca weryfikacji mogła określić, do których danych odnosi się podpis elektroniczny;
 4. aby osoba dokonująca weryfikacji mogła określić, któremu sygnatariuszowi został przydzielony dany podpis elektroniczny oraz czy został użyty pseudonim sygnatariusza;
 5. aby można było rozpoznać zmiany w danych opatrzonych podpisem, które pociągają za sobą implikacje dla zabezpieczeń.
- (5) Środki techniczne i procedury używane do tworzenia bezpiecznych podpisów muszą być stale w odpowiedni sposób weryfikowane, z wykorzystaniem aktualnych w danym czasie rozwiązań technicznych. Zgodność z wymaganiami w zakresie zabezpieczeń musi być potwierdzona przez instytucję zatwierdzającą, o której mówi § 19.

§ 19

Instytucja zatwierdzająca

- (1) Obowiązki spoczywające na instytucji zatwierdzającej wynikające z niniejszej ustawy i z rozporządzeń wydanych na jej podstawie mogą być wypełniane wyłącznie przez instytucję odpowiednio do tego celu przygotowaną.
- (2) Instytucja może wypełniać obowiązki spoczywające na instytucji zatwierdzającej, jeśli:
 1. wykaże, że zapewnia wymaganą niezawodność;
 2. zatrudnia rzetelnych pracowników dysponujących specjalistyczną wiedzą, doświadczeniem i kwalifikacjami, a w szczególności wiedzą w zakresie podpisów elektronicznych, odpowiednich procedur zabezpieczeń, kryptografii, technologii komunikacyjnej oraz technologii kart inteligentnych, którzy to pracownicy potrafią korzystać ze środków technicznych niezbędnych do wypełniania obowiązków spoczywających na instytucji zatwierdzającej;
 3. posiada wystarczające wyposażenie techniczne i zasoby oraz jest w odpowiednim stopniu wypłacalna;
 4. gwarantuje wymaganą niezależność, neutralność i bezstronność.
- (3) Kanclerz Federalny postanowi w rozporządzeniu wydanym w porozumieniu z Ministrem Sprawiedliwości, że dana instytucja może stać się instytucją zatwierdzającą. Takie rozporządzenie będzie wydane wyłącznie na prośbę zainteresowanej instytucji i tylko w sytuacji, gdy instytucja spełnia wymagania określone w ust. (2), który dotyczy jej statutu, organizacji, bezpieczeństwa i spraw finansowych.
- (4) Instytucja zatwierdzająca może otrzymać raporty testowe na temat środków technicznych i procedur od innych instytucji i agencji, aby mogła wypełniać spoczywające na niej obowiązki wynikające z niniejszej ustawy i rozporządzeń wydanych na jej podstawie.

Rozdział 6

Prawa i obowiązki użytkowników

§ 20

Powszechny obowiązek udzielania informacji przez usługodawcę certyfikacyjnego

- (1) Przed zawarciem kontraktu usługodawca certyfikacyjny na piśmie lub przy użyciu trwałego nośnika danych udzieli wnioskodawcy starającemu się o uzyskanie certyfikatu jasnych i wyczerpujących informacji na temat reguł bezpieczeństwa i certyfikacji. Przy wydawaniu certyfikatów kwalifikowanych usługodawca certyfikacyjny poinformuje również posiadacza certyfikatu o warunkach użycia takiego certyfikatu, takich jak ograniczenie zakresu certyfikatu lub wartości transakcji, oraz poinformuje go o dobrowolnej akredytacji, o której mowa w § 17, a także wszelkich specjalnych procedurach rozstrzygnięcia sporów.
- (2) Informacje, o których mowa w ust. (1), będą również udostępnione na prośbę strony trzeciej, która może udowodnić, że posiada domniemany interes prawny do takich informacji.
- (3) Usługodawca certyfikacyjny udzieli posiadaczowi certyfikatu informacji na temat środków technicznych i procedur odpowiednich dla używanej procedury składania podpisu elektronicznego i ewentualnie informacji na temat środków technicznych, procedur i innych urządzeń zgodnych z wymaganiami dotyczącymi tworzenia i weryfikacji podpisów elektronicznych. Ponadto posiadacz certyfikatu musi otrzymać informacje na temat możliwych skutków prawnych używanej procedury składania podpisu elektronicznego, obowiązków sygnatariusza oraz szczególnej odpowiedzialności usługodawcy certyfikacyjnego. Posiadacz certyfikatu musi również otrzymać informacje, że należy użyć nowego podpisu elektronicznego (i ewentualnie informacje, jak należy to zrobić), zanim wartość zabezpieczająca aktualnego podpisu ulegnie znacznemu obniżeniu.

§ 21

Obowiązki sygnatariusza

Sygnatariusz musi wykazywać odpowiednią dbałość o dane do tworzenia podpisu, w maksymalnym możliwym zakresie zapobiegać nieupoważnionemu dostępowi do nich oraz ich nie przekazywać. Sygnatariusz zażąda unieważnienia certyfikatu w przypadku zagubienia danych do tworzenia podpisu, uzasadnionego podejrzenia ich naruszenia lub zmiany faktów potwierdzonych certyfikatem.

§ 22

Ochrona danych

- (1) Usługodawca certyfikacyjny będzie korzystać wyłącznie z danych osobowych niezbędnych do świadczenia swoich usług. Dane te mogą zostać uzyskane wyłącznie od zainteresowanej osoby lub, za jej zgodą, od strony trzeciej.
- (2) Jeżeli używany jest pseudonim, usługodawca certyfikacyjny udzieli informacji o danych osobowych sygnatariusza, o ile będzie istnieć oparty na domniemaniu faktycznym dowód uzasadnionego interesu prawnego w ustaleniu jego tożsamości zgodnie z § 8 ust. (1) punkt 4 i ust. (3) Ustawy o Ochronie Danych Osobowych. Fakt udzielania informacji musi zostać zarejestrowany.
- (3) Postanowienia powyższe nie wpływają na obowiązek udzielenia informacji i pomocy sądom oraz innym władzom przez usługodawcę certyfikacyjnego.

§ 23

Odpowiedzialność organu certyfikacyjnego

- (1) Usługodawca certyfikacyjny, który wydaje certyfikaty kwalifikowane lub występuje jako gwarant takich certyfikatów zgodnie z § 24 ust. (2) punkt 2, jest odpowiedzialny wobec osób pokładających zaufanie w certyfikacie za zapewnienie, aby:
 1. certyfikat kwalifikowany zawierał dokładne informacje w momencie wydania,
 2. sygnatariusz, który jest posiadaczem certyfikatu kwalifikowanego, posiadał dane do tworzenia podpisu odpowiadające danym do weryfikacji podpisu umieszczonym na certyfikacie w momencie jego wydania,

3. dane do tworzenia podpisu i odpowiadające im dane do weryfikacji podpisu były zgodne, kiedy produkty i procedury dostarczane lub zalecane przez usługodawcę certyfikacyjnego są używane razem,
 4. certyfikat został bezzwłocznie unieważniony, jeśli zaistnieje powód ku temu i będą dostępne usługi unieważniania,
 5. w celu wygenerowania i przechowywania danych do tworzenia podpisu zostały spełnione wymagania określone w § 7 oraz użyte środki techniczne i procedury określone w § 18.
- (2) Usługodawca certyfikacyjny, który dostarcza procedury składania zabezpieczonych podpisów elektronicznych, będzie również odpowiedzialny za zapewnienie, aby dostarczane lub zalecane przez niego produkty, procedury i inne środki do tworzenia podpisów elektronicznych i uwidaczniania danych opatrzonych podpisem korzystały wyłącznie ze środków technicznych i procedur określonych w § 18.
 - (3) Usługodawca certyfikacyjny nie będzie ponosić odpowiedzialności, jeśli będzie w stanie dowieść, że ani on, ani jego pracownicy nie są winni naruszenia obowiązków określonych w ust. (1) i (2). Jeśli poszkodowana strona może wykazać, że istnieje prawdopodobieństwo naruszenia obowiązków określonych w ust. (1) i (2) lub środków podjętych w celu spełnienia wspomnianych wyżej wymagań, przyjęte zostanie założenie, że jest to przyczyna poniesionych szkód. Założenie to zostanie odrzucone, jeśli usługodawca certyfikacyjny będzie mógł wykazać, że istnieje prawdopodobieństwo, iż szkody nie zostały spowodowane naruszeniem obowiązków i środków, o których mowa w ust. (2).
 - (4) Jeśli zakres certyfikatu kwalifikowanego jest ograniczony, usługodawca certyfikacyjny nie będzie ponosić odpowiedzialności za szkody wynikłe z niezastosowania się do tego ograniczenia w czasie używania certyfikatu. Jeśli certyfikat kwalifikowany podaje określoną wartość transakcji, której nie należy przekraczać, usługodawca certyfikacyjny nie będzie ponosić odpowiedzialności za szkody wynikłe z powodu przekroczenia tej wartości.
 - (5) Odpowiedzialność usługodawcy certyfikacyjnego określona w ust. (1), (2) i (3) nie może zostać wyłączona ani ograniczona z góry.
 - (6) Bez zmiany pozostają przepisy Austriackiego Kodeksu Cywilnego oraz pozostałe przepisy, które stanowią, że poniesione szkody mają zostać zrekompensowane w innym stopniu lub przez inne osoby.

Rozdział 7

Uznawanie certyfikatów wydawanych w innych państwach

§ 24

Uznawanie

- (1) Certyfikat wydany przez usługodawcę certyfikacyjnego mającego siedzibę w kraju Wspólnoty Europejskiej [w paragrafie tym są używane wymiennie terminy **European Community i European Union; naszym zdaniem w każdym przypadku powinno być European Union (Unia Europejska) – przyp. BTInfo**], którego ważność może zostać zweryfikowana w Austrii, będzie równoważny certyfikatowi wydanemu w Austrii. Certyfikat kwalifikowany wydany przez wspomnianego wyżej usługodawcę certyfikacyjnego będzie powodował takie same skutki prawne, jak certyfikat kwalifikowany wystawiony w Austrii.
- (2) Certyfikat wystawiony przez usługodawcę certyfikacyjnego mającego siedzibę w kraju nienależącym do Wspólnoty Europejskiej, którego ważność może zostać zweryfikowana w Austrii, zostanie uznany w Austrii. Certyfikat kwalifikowany będzie równoważny certyfikatowi wydanemu w Austrii, jeśli spełnione będą następujące warunki:
 1. usługodawca certyfikacyjny spełnia postanowienia określone w § 7 i jest akredytowany w ramach dobrowolnego systemu akredytacji w kraju należącym do Unii Europejskiej;
 2. usługodawca certyfikacyjny mający siedzibę w kraju Wspólnoty Europejskiej, który spełnia postanowienia określone w § 7, występuje jako gwarant certyfikatu zgodnie z przepisami prawa cywilnego;
 3. certyfikat jest uznany za certyfikat kwalifikowany lub usługodawca certyfikacyjny jest uznany jako organ wydający certyfikaty kwalifikowane na podstawie dwu- lub wielostronnej umowy zawartej przez Wspólnotę Europejską z krajami trzecimi lub organizacjami międzynarodowymi.
- (3) Jeśli w kraju należącym do Unii Europejskiej lub innym został utworzony uznawany przez rząd organ mający udowodnić, że spełnione zostały wymagania w zakresie

zabezpieczeń dla bezpiecznego podpisu elektronicznego, certyfikat wydany przez wspomniany wyżej organ, który potwierdza zgodność z wymaganiami w zakresie zabezpieczeń regulujących tworzenie bezpiecznych podpisów elektronicznych, będzie równoznaczny z certyfikatem wydanym przez instytucję zatwierdzającą, o której mowa w § 19, o ile organ nadzorczy ustali, że wymagania techniczne, kontrole i procedury testowe, na podstawie których wspomniany wyżej organ opiera swoją ocenę, odpowiadają wymaganiom technicznym, kontroli i procedurom testowym stosowanym przez instytucję zatwierdzającą.

Rozdział 8

Postanowienia końcowe

§ 25

Rozporządzenie dotyczące podpisu elektronicznego

Kanclerz Federalny wyda w porozumieniu z Ministrem Sprawiedliwości rozporządzenia niezbędne do wejścia w życie niniejszej ustawy zgodnie z aktualnym stanem nauki i techniki.

Rozporządzenia te określają:

1. wysokość jednolitych stawek opłat pokrywających koszty usług świadczonych przez organ nadzorczy oraz Telecom-Control GmbH, wraz z ustaleniem, w jaki sposób będzie się je pobierać;
2. poziom zasobów finansowych wymaganych, aby spełnić wymagania niniejszej ustawy i rozporządzeń wydanych na jej podstawie oraz pokryć ryzyko odpowiedzialności cywilnej usługodawcy certyfikacyjnego, wraz z ustaleniem minimalnej sumy ubezpieczenia od odpowiedzialności cywilnej;
3. kwalifikacje usługodawcy certyfikowanego i jego pracowników, o których mowa w § 7 ust. (1) i § 14 ust. (2);
4. wymagania dotyczące środków technicznych, procedur, produktów technicznych i innych zasobów wymaganych, aby spełnić § 7 ust. (2), § 10 i § 18, metodę kontroli środków technicznych i procedur zgodnie z § 18 oraz metodę wydawania potwierdzenia zgodności z tymi wymaganiami;
5. okres, przez jaki kontynuacja usług unieważniania musi być prowadzona przez organ nadzorczy, o czym mówi § 12 i § 14 ust. (5).

6. zakres wymagań i granice tolerancji dla bezpiecznych datowników;
7. okres ważności i przedłużenia ważności certyfikatów kwalifikowanych oraz termin i procedurę dołączania nowego podpisu elektronicznego (kolejny podpis);
8. formę, przedstawienie i dostępność reguł certyfikacji (np. tekst w postaci niezaszyfrowanej);
9. okres, przez jaki należy przechowywać informacje w rejestrach, o których mowa w § 11;
10. format opisu akredytowanych usługodawców certyfikacyjnych.

§ 26

Postanowienia administracyjne

- (1) Każda osoba, która bezprawnie posługuje się danymi do tworzenia podpisu należącymi do innej osoby bez wiedzy i zgody sygnatariusza, popełnia wykroczenie zagrożone grzywną w wysokości do 56 000 szylingów austriackich.
- (2) Usługodawca certyfikacyjny popełnia wykroczenie zagrożone grzywną w wysokości do 112 000 szylingów austriackich, jeśli:
 1. narusza obowiązek unieważnienia certyfikatu, postępując wbrew postanowieniom § 9 ust. (1);
 2. narusza obowiązek prowadzenia rejestrów, postępując wbrew postanowieniom § 11;
 3. odmawia wglądu do ksiąg, rejestrów i dokumentacji określonych w § 16 ust. (1) lub nie udziela wymaganej informacji, postępując wbrew postanowieniom § 16 ust. (1);
 4. nie udziela informacji posiadaczowi certyfikatu, postępując wbrew postanowieniom § 20 ust. (1) i (3).
- (3) Usługodawca certyfikacyjny popełnia wykroczenie zagrożone grzywną w wysokości do 224 000 szylingów austriackich, jeśli:
 1. nie powiadamia o rozpoczęciu działalności lub nie przedkłada reguł zabezpieczenia i certyfikacji, postępując wbrew postanowieniom § 6 ust. (2);
 2. nie powiadamia organu nadzorczego o wszelkich faktach uniemożliwiających dalsze prowadzenie działalności we właściwy sposób w zgodzie z ideą bezpieczeństwa i certyfikacji, postępując wbrew postanowieniom § 6 ust. (5);

3. nie świadczy odpowiednich usług katalogowania i unieważniania, postępując wbrew postanowieniom § 7 ust. (1) punkt 2;
 4. nie podejmuje odpowiednich środków, aby uniemożliwić usługodawcy certyfikacyjnemu lub stronom trzecim kopiowanie lub przechowywanie danych do tworzenia podpisu należących do sygnatariusza, postępując wbrew postanowieniom § 7 ust. (1) punkt 8;
 5. nie używa, nie dostarcza ani nie poleca odpowiednich środków technicznych i procedur do składania bezpiecznych podpisów elektronicznych, postępując wbrew postanowieniom § 18;
 6. nie zaprzestaje działalności pomimo zakazu wydanego przez organ nadzorczy, o czym mówi § 14 ust. (2), (3) i (4).
- (4) Nie zostaje popełnione wykroczenie określone w ust. (1), (2) i (3), jeśli dany czyn stanowi przestępstwo, które może być ścigane sędownie lub podlega surowszym sankcjom na podstawie innych przepisów administracyjnych.
- (5) Jeśli zostanie stwierdzone przestępstwo kryminalne, może nastąpić przepadek przedmiotów użytych do jego popełnienia.

§ 27

Wejście w życie i odniesienia

- (1) Niniejsza ustawa wchodzi w życie z dniem 1 stycznia 2000 r.
- (2) Zawarte w treści niniejszej ustawy odniesienia do przepisów innych ustaw federalnych dotyczą ich obecnie obowiązujących wersji.

§ 27

Wykonanie

Następujące osoby będą odpowiedzialne za wprowadzenie w życie niniejszej ustawy:

1. §§ 3, 4 i 23: Minister Sprawiedliwości;
2. §§ 13 do 17: Minister Nauki i Transportu;
3. §§ 22 i 26: Kanclerz Federalny;
4. §§ 7 ust. (1) punkt 6 i 13 ust. (4): Kanclerz Federalny w porozumieniu z Ministrem Sprawiedliwości i Ministrem Finansów;

5. pozostałe przepisy: Kanclerz Federalny w porozumieniu z Ministrem Sprawiedliwości.