

[CZ] Electronic Signature Act

IRIS 2000-9:1/31

Jan Fučík
Česká televize

The Czech Republic has become the first country in Central and Eastern Europe to pass a law on electronic signatures. The Czech Parliament adopted the Zákon c. o elektronickém podpisu (Electronic Signature Act) on 29 June 2000 in order to transpose Directive 1999/93/EC into domestic law.

The Act contains definitions that correspond with those set out in the EC Directive. An "electronic signature" is defined as data in electronic form which are attached to or logically associated with other electronic data and which serve as a method of authentication. An "advanced electronic signature", which offers a higher degree of security, must meet a series of more stringent requirements. A "signatory" is a natural person who holds an electronic signature-creation device and acts either on his own behalf or on behalf of another natural or legal person. A "certificate" is an electronic attestation which links signature-verification data to a natural person and confirms the identity of that person. "Qualified certificates" are defined as electronic attestations which meet the requirements laid down in the Act and are provided by certification service providers who fulfil the requirements of the Act.

A "certification service provider" is the legal or natural person who issues certificates, keeps a record of them or provides other services related to electronic signatures. "Accredited certification service providers" are accredited under the terms of the Act. All qualified certificates should meet certain requirements and contain the advanced electronic signature of the certification service provider.

Certification service providers do not need to be officially approved.

Certification service providers issuing qualified certificates should be registered as such with the regulatory authority and fulfil the requirements of the Act.

Accredited certification service providers which cease their operations must inform the regulatory authority as early as possible (no later than three months after ceasing operations). They must either ensure that valid certificates are taken over by another certification service provider or invalidate them.

The regulatory authority can use a range of measures, including fines, to enforce these requirements. For monitoring purposes, certification service providers must

allow the various organs of the regulatory authority access to their business premises. They must also, on request, make available any relevant documentation, even if it only exists in electronic format, and offer any assistance that may be necessary. The tasks of the regulatory authority are performed by the Data Protection Office.

Foreign certificates may be used as qualified certificates provided they are recognised as such by a certification service provider entitled to issue qualified certificates under the terms of the Act. Such a provider must guarantee the accuracy and validity of the foreign certificate.

The regulatory authority is empowered to issue decrees on the implementation of the Act.

Through the adaptation of the relevant provisions, electronic signatures are recognised under civil, administrative (fiscal) and criminal law.

The Act will enter into force three months after being published in the Gazette of Laws and Decrees of the Czech Republic, i.e. on 26 October 2000.

***Zákon o elektronickém podpisu a o změně některých dalších zákonů
(zákon o elektronickém podpisu), 29.06.2000***

Electronic Signature Act, 29 June 2000

