ELECTRONIC SIGNATURE AND AMENDMENTS TO CERTAIN OTHER LEGISLATION REPÚBLICA CHECA

- PART ONE. ELECTRONIC SIGNATURE **1**
- PART TWO. AMENDMENTS TO THE CIVIL CODE **11**
- PART THREE. AMENDMENTS TO ACT No. 337/1992 Coll., ON ADMINISTRATION OF TAXES AND FEES **11**
- PART FOUR. AMENDMENTS TO THE ADMINISTRATION CODE **12**
- PART FIVE. AMENDMENTS TO THE RULES OF COURT **12**
- PART SIX. AMENDMENTS TO THE PENAL CODE **12**
- PART SEVEN. AMENDMENTS TO THE PERSONAL DATA PROTECTION ACT **13**
- PART EIGHT. AMENDMENTS TO THE ACT ON ADMINISTRATIVE FEES **13**
- PART XII. PROCEEDINGS UNDER THE ELECTRONIC SIGNATURE ACT **13**
- PART XII. PROCEEDINGS UNDER THE ELECTRONIC SIGNATURE ACT ITEM 162 ..... **14**
- PART NINE. THE ACT COMES INTO FORCE AND EFFECT ON THE FIRST DAY OF THE THIRD CALENDAR MONTH FOLLOWING PROMULGATION DATE **14**

ACT 227 OF JUNE 29, 2000

ELECTRONIC SIGNATURE AND AMENDEMENTS TO CERTAIN OTHER LEGISLATION REPÚBLICA CHECA

The Parliament of the Czech Republic has passed the following legislation:

PART ONE. ELECTRONIC SIGNATURE ➦

Article 1.- The Purpose of the Act

The legislation regulates the application of electronic signature, the rendition of related services, the enforcement of obligations set forth by the Act, and the penalization of violations of the obligations stipulated by the Act.

Article 2.- Definition of Certain Terms

For the purposes of the Act, it applies that:

a) an electronic signature is information in electronic form, attached to a data statement or logically related thereto, which enables its recipient to verify the identity of the undersigned;

b) a guaranueed electronic signature is a signature which satisfies the following requirements:

1) it is clearly linked to the undersigned;

2) it provides for the identification of the undersigned in respect of the data statement;

3) it is created and attached to the data statement with the aid of means which are solely controlled by the undersigned;

4) is attached to the respective data statement in a manner which enables its recipients to detect any and all subsequent data alteration;

c) a data statement means electronic data which can be transferred by electronic communication means and stored in data carriers used for electronic data processing and transmission;

d) the undersigned is a physical person who has the means to create an electronic signature and who acts on its own behalf or on behalf of another physical or legal entity;

e) a provider of certification services is an entity that issues certificates and keeps record thereof, and may provide other services related to electronic signatures;

f) an accredited provider of certified services is a provider of certification services on the basis of accreditation granted in accordance with this Act;

g) a certificate is a data statement issued by the provider of certification services, which links identity verification data with the undersigned as part of the identity verification process;

h) a qualified certificate is a certificate comprising all the particulars stipulated by the Act; it is issued by the provider of certification services which must satisfy all the conditions stipulated by the Act applicable to providers of certification services authorized to issue qualified certificates;

i) data used for the creation of electronic signatures are specific data which the undersigned uses for creating electronic signatures;

j) data used for the verification of electronic signatures are specific data used for verifying electronic signatures;

k) means for the creation of electronic signatures are technical devices or software programs which the undersigned uses for creating electronic signatures;

l) means for the verification of electronic signatures are technical devices or software programs used for verifying electronic signatures;

m) means for secure creation of electronic signatures are means used for creating electronic signatures, which meet the requirements stipulated by the Act;

n) means for secure verification of electronic signatures are means used for verifying electronic signatures, which meet the requirements stipulated by the Act;

o) electronic signature instruments are technical devices or software programs, or parts thereof, used in the rendition of certification services or for the creation or verification of electronic signatures;

p) an accreditation certificate means that the provider of certification services meets the requirements stipulated by the Act, applicable to providers of certification services.

Article 3.- Compliance with Signature Requirements

(1) A data statement is signed, if provided with an electronic signature.

(2) The application of a guaranteed electronic signature, based on a qualified certificate and secured signature creation, enables the recipient to verify whether a data statement has been signed by the person specified in the qualified certificate.

Article 4.- Compliance with the Original

A guaranteed electronic signature means that any adulteration of the contents of an undersigned data statement can be traced from the point of signature.

Article 5.- Obligations of the Signatory

(1) The signatory is obliged to:

a) handle the means, as well as the data used for the creation of a guaranteed electronic signature with a duly care to prevent their abuse;

b) notify the provider of certified services and issuer of its qualified certificate, without undue delay, if danger of abuse occurs in respect of the data that the signatory uses for the creation of a guaranteed electronic signature;

c) to provide the provider of certification services with accurate, true, and complete information on matters pertaining to the qualified certificate.

(2) The signatory shall be held liable for any violation of the obligations specified in Paragraph 1 herein above to the extent of special legislation.1) However, if the signatory proves that the damaged party failed to perform all the procedures necessary to verify the validity of the guaranteed electronic signature, his liability shall be waived, provided that his qualified certificate has not been invalidated.

Article 6.- Obligations of the Provider of Certification Services and Issuer of Qualified Certificates

(1) Providers of certification services and issuers of qualified certificates are obliged:

a) to ensure that all the certificates they issue as qualified certificates have all the particulars required under the Act for qualified certificates;

b) to ensure that all data specified in qualified certificates are accurate, true, and complete;

c) to verify the identity of the recipients of qualified certificates prior to issue, using relevant means of identification, including special identification symbols, if it is deemed necessary

for the purposes of the given qualified certificate;

d) to establish, at the time of issue of the qualified certificate, whether the signatory's data for creating electronic signatures corresponded with the data for verifying electronic signatures, contained in the qualified certificate;

e) to ensure that everyone would be able to verify the identity of the provider of certification services and its qualified certificate;

f) to compile and operate a well-secured list of qualified certificates, accessible to the public even on a long-distance basis, and to update it on a current basis;

g) to operate a well-secured and publicly accessible list of invalidated qualified certificates, even on a long-distance basis;

h) to ensure that the date and time of issue and/or invalidation of qualified certificates – including the hour, minute, and second – can be exactly determined and this information be accessible to third parties;

i) to hire or contract professional persons with specialized knowledge, experience, and qualifications to provide certification services, and to ensure that such persons be well acquainted with relevant security procedures;

j) to use security systems and electronic signature instruments, as well as adequate security procedures to support these systems and instruments; an electronic signature instrument is considered secure if it satisfies all the requirements stipulated by the Act and the relevant rules of procedure; this must be verified by the Office for Personal Data Protection (hereinafter "The Office");

k) to adopt adequate measures against the possibility of abuse or forgery of qualified certificates and for the protection of the data used in the creation of guaranteed electronic signatures, if the provider's services include the creation thereof;

l) to dispose of sufficient financial resources, in accordance with the requirements stipulated by the Act and with consideration to liability risks;

m) to keep all information and documentation on each qualified certificate issued, for at least 10 years following the expiry of the qualified certificate's validity; both the information and documentation may be stored in electronic form;

n) to inform applicants for a qualified certificate, prior to entering contractual relations with them, of the exact conditions applicable to the use of qualified certificates, including limitations thereof; and to inform them whether or not they have been accredited by The Office under the provisions of Section 10 hereof; and to disclose a substantial portion of this information to third parties relying on the given qualified certificate;

o) to use a secure system for the storage of qualified certificates so that entries and amendments thereto could be made by authorized persons only, the accuracy of entries could be verified, and any and all technical or program alterations violating these security requirements could be easily detected.

(2) The provider of certification services and issuer of qualified certificate issues qualified certificates to signatories on a contractual basis. The contract must be executed in writing to be valid.

(3) The provider of certification services and issuer of qualified certificates must not store or copy data used for the creation of guaranteed electronic signatures of persons who contract services from the provider of certification services.

(4) In the event that The Office withdraws accreditation from a provider of certification services and issuer of qualified certificates, the provider is obliged to notify of this circumstance all the persons who contract services from this provider and disclose this circumstance in the list specified in Paragraph 1(f,g) herein above.

(5) Providers of certification services that are not accredited by The Office and intend to issue qualified certificates are obliged to report their intention to The Office no later than 30 days prior to issuing the first qualified certificate.

(6) In the event that a provider of certification services and issuer of qualified certificates specifies limitations on the use of the certificate, including limitation on the amount of transaction for which the qualified certificate can be applied, the limitations must be apparent to third parties.

(7) The provider of certification services and issuer of qualified certificates must terminate the validity of a qualified certificate, if the signatory so demands or if it is established that the certificate was issued on basis of false or inaccurate information.

(8) Furthermore, the provider of certification services and issuer of qualified certificates must terminate the validity of a qualified certificate, if it establishes that the signatory has died or been declared legally incompetent, fully or partly,2) or if the data used for the issue of the certificate become invalid.

(9) Providers of certification services and issuers of qualified certificates must keep documentation of its operations, which must contain:

a) contracts with signatories on the issue of qualified certificates;

b) the qualified certificates issued to date;

c) copies of personal data submitted by signatories;

d) confirmation of acceptance of a qualified certificate from each signatory;

e) exact time of the qualified certificate’s validity.

(10) The employees of a provider of certification services and issuer of qualified certificates, or other physical persons who come into contact with personal information and data used for the creation of electronic signatures by signatories, are obliged to observe the rule of confidentiality in respect of the personal information, data, and security measures used for and involved in the creation of electronic signatures, as their disclosure would jeopardize the security of the information and data used for the creation of electronic signatures. This obligation prevails even after ending the employment or the given work assignment.

Article 7. Professional Liability

(1) Providers of certification services and issuers of qualified certificates are liable for violations of their obligations stipulated by the Act, to the extent of special legislation.1)

(2) Providers of certification services and issuers of qualified certificates are not liable for losses caused by failure to comply with limitations on its use.

Article 8.- Personal Data Protection

Protection of personal data is subject to special legal provisions. 3)

Article 9.- Accreditation and Supervision

(1) The Office is the sole authority empowered to issue accreditation to providers, thus authorizing them to render certification services, and to enforce adherence to the provisions of the Act.

(2) The Office:

a) grants and withdraws accreditation to/from providers of accredited certification services in the territory of the Czech Republic;

b) supervises the activities of accredited providers of certification services and issuers of qualified certificates, imposes remedial measures on them, as well as penalties for non-compliance with obligations stipulated by the Act;

c) keeps record of accreditation's issued to date and amendments thereto, and of those providers of certification services that have notified The Office that they issue qualified certificates;

d) publishes a list of accreditation's issued to date, regularly, and a list of accredited providers of certification services and issuers of qualified certificates; these announcements must be accessible on a long-distance basis;

e) fulfils other obligations stipulated by the Act and the relevant rules of procedure;

f) fulfils other obligations stipulated by the Act (e.g., Sec. 10(7), Sec. 13(2) and Sec. 16(2).

(3) For the purposes of supervision, accredited providers of certification services and issuers of qualified certificates are obliged to allow, to the extent necessary, authorized employees of The Office to enter their commercial premises and operations, examine - upon request - any and all documentation, records, documents, correspondence, and other papers related to their activities, facilitate access, to the extent necessary, to their information systems, and provide them with all the information and co-operation necessary.

(4) Unless otherwise stipulated in the Act, The Office shall perform supervision in accordance with special legislation. 4)

Article 10.- Conditions of Granting Accreditation to Providers of Certification Services

(1) Every provider of certification services may file an application with The Office for a permit to become an accredited provider of certification services. Filing an application for accreditation is subject to an administrative fee.5)

(2) An application for accreditation must have the following particulars:

a) the registered title, address, and identification number of the applicant;

b) the applicant's trade license and, for entities registered in the Commercial Register, also a transcript from the Commercial Register, not older than 3 months;

c) a transcript from the Crime Register, if a physical person or statutory proxy of a legal entity, in the event that the applicant is a legal entity, not older than 3 months;

d) material, personal, and organizational prerequisites applicable to providers of certification services and issuers of qualified certificates, in accordance with Sec. 6 of the Act;

e) information as to whether the applicant issues or intends to issue qualified certificates;

f) a proof of payment of the administrative fee.

(3) In the event that the application does not contain all the required particulars, The Office shall interrupt the proceedings and ask the applicant to complement the missing part(s) within a certain time limit. If the applicant fails to comply, The Office shall arrest the proceedings. The administrative fee shall not be refunded.

(4) If the applicant meets all the accreditation conditions required by the Act, The Office shall pass a decision to grant the accreditation. In the opposite event, the application for accreditation shall be rejected.

(5) Accredited providers of certification services must be registered in the territory of the Czech Republic.

(6) Apart from activities specified in the Act, accredited providers of certification services may act as attorneys, notaries, and court-certified experts;6) all other activities are subject to a prior consent from The Office.

(7) Verification of the qualified certificate of applicant and provider of certification services, by The Office, forms an integral part of The Office's decision to grant an accreditation.

Article 11.-

Public administration authorities shall accept only guaranteed electronic signatures and qualified certificates issued by accredited providers of certification services.

Article 12.- Qualified Certificate Particulars

(1) A qualified certificate must contain:

a) a note stating that it has been issued as a qualified certificate in accordance with the Act;

b) the registered title and address of the provider of certification services, and information stating that the certificate has been issued in the Czech Republic;

c) the first name and surname of the signatory or his pseudonym, with a note stating that it is a pseudonym;

d) special symbols of the signatory, if so required for the purposes of a qualified certificate;

e) data for verification of the signature; these data must correspond with the data used for the creation of electronic signatures which are specific to the undersigned;

f) a guaranteed electronic signature of the provider of certification services and issuer of qualified certificates;

g) number of the qualified certificate which is unique for the specific provider of certification services;

h) the commencement and expiry of the effective period of the qualified certificate;

i) information specifying that the use of the qualified certificate is subject to limitations in respect of the type or extent of use, if applicable;

j) information specifying that the qualified certificate is subject to a limitation on the amount of transaction, if applicable.

(2) Qualified certificate may contain other personal data only with the consent of the signatory.

Article 13.- Obligations of Accredited Providers of Certification Services after Termination of Activities

(1) Accredited providers of certification services must notify The Office of their intent to terminate their activities at least 3 months in advance and make every effort to transfer the valid qualified certificates to another accredited provider of certification services. Furthermore, accredited providers of certification services must notify the signatories, which contract their services, of their intent to terminate their activities at least 2 months in advance.

(2) Accredited providers of certification services that are unable to find another accredited provider of certification services as their successor must notify The Office of this circumstance in a timely manner. Upon receiving such notification, The Office takes over the list of accredited qualified certificates issued to date and notifies the respective signatories accordingly.

(3) The provisions of Paragraphs 1 and 2 herein above shall apply as deemed appropriate also in the event that the given accredited provider of certification services is dissolved, dies, or ceases to conduct its activities, without meeting its reporting obligation in accordance with Paragraph 1 herein above.

Article 14.- Remedial Measures

(1) In the event that The Office establishes that an accredited provider of certification services or a provider of certification services violates its obligations stipulated by the Act, The Office orders the provider to remedy the situation within a certain time limit; The Office may determine what measures would this provider of certification services be obliged to take.

(2) In the event that an accredited provider of certification services commits a more severe violation of its obligations or fails to do so within the time limit, The Office shall have the right to withdraw accreditation from this provider.

(3) If The Office decides to withdraw accreditation from an accredited provider of certification services, the Office may also invalidate the qualified certificates issued by the provider of certification services during the accreditation period.

Article 15.- Invalidation of Qualified Certificates

(1) The Office may order a provider of certification services to invalidate a signatory's qualified certificate, as a preliminary measure,7) if a well-founded prejudice exists to suspect that the given qualified certificate is forged or has been issued on the basis of false information. An order to invalidate may also be issued in the event that the means that the signatory uses for the creation of electronic signatures show to have security flaws which could facilitate forging of electronic signatures or alteration thereof.

(2) The list of certificates specified in Sec. 6(1g) must indicate the exact time of the certificate's invalidation. Invalidated certificates must not be permitted be renewed or used again.

Article 16.- Honouring Foreign Certificates

(1) Certificates issued by a foreign provider of certification services, which are considered qualified under the terms of the Act, may be used as qualified certificates, if honoured as such by a provider of certification services that issues qualified certificates in accordance with the Act, and under the condition that this provider of certification services guarantees the accuracy and validity of the foreign qualified certificates to the same extent as its own qualified certificates.

(2) Certificates issued by a foreign provider of certification services as qualified certificates, under the terms of the Act, can be honoured as qualified certificates, if so recognized by a decision of The Office or under the terms of international conventions, or if an agreement on bilateral recognition of certificates is entered between a foreign authority competence or a foreign provider of certification services and The Office.

Article 17.- Means Used for Secure Creation and Verification of Guaranteed Electronic Signatures

(1) The means for secure creation of electronic signatures is a set of certain technical and program facilities and procedures that must ensure at least that:

a) the data used for the creation of electronic signatures occur only once and their security is duly assured;

b) the data used for the creation of electronic signatures are sufficiently secured to eliminate the possibility of deduction by persons familiar with the mode and means of their creation, and adequately protected against forgery with the aid of state-of-the-art technology;

c) the data used for the creation of electronic signatures are properly protected against abuse by a third party.

(3) The means used for the creation of electronic signatures must not modify the data used for signing or prevent them from being presented to the signatory before signing.

(4) The means for secure verification of electronic signatures is a set of certain technical

and program facilities and procedures that must ensure at least that:

a) the data used for the verification of electronic signatures correspond with the data presented to the signatory before signing;

b) the signature is reliably verified and the result of the verification duly displayed;

c) the verifier can reliably to verify the contents of the undersigned data;

d) the verity and validity of the certificate can be reliably verified;

e) the results of the verification and the identity of the signatory must be duly displayed;

f) the use of a synonym must be indicated clearly;

g) all alterations jeopardizing security can be detected.

Article 18.- Penalties

(1) The Office may impose a penalty of up to CZK 10,000,000 to accredited providers of certification services or providers of certification services and issuers of qualified certificates for violating their obligations stipulated by the Act.

(2) In the event that an accredited provider of certification services or provider of certification services and issuer of qualified certificates commits another violation of its obligations stipulated by the Act within one year of penalization, The Office may impose a penalty of up to CZK 20,000,000.00.

(3) Accredited providers of certification services or providers of certification services and issuers of qualified certificates who hamper The Office in its supervision activities may be imposed a penalty of up to CZK 1,000,000.00 for each violation.

(4) Persons who fail duly to cooperage with The Office during its supervision activities may be imposed a penalty of up to CZK 25,000.00 for each violation of this duty.

(5) In its decision-making on the amount of penalty, The Office takes into consideration especially the manner of such conduct, the degree of fault, the gravity of the violation, the extent and duration thereof, and the consequences of the unlawful conduct.

(6) The penalty may be imposed up to one year, but no later than three years, from the day of detection.

(7) The Office collects penalties. Penalties are solicited by the financial institution of competence by venue, in accordance with special legislation. 8)

(8) Penalties constitute revenues to the state budget of the Czech Republic.

Article 19.-

Unless otherwise stipulated in the Act, proceedings arising from the Act are subject to special legislation.9)

Article 20.- Authorization Provisions

The Office is authorized to issue decrees further specifying the provisions of Section 6 and 17 hereof and the manner proving adherence thereto; and further specifying the requirements on the instruments used for electronic signatures; and further specifying the particulars of the process and manner of assessing compliance of electronic signature instruments with these requirements.

PART TWO. AMENDMENTS TO THE CIVIL CODE ➦

Article 21.-

Act No. 40/1964 Coll., the Civil Code, as subsequently amended by Act No. 58/1969 Coll., Act No. 131/1982 Coll., Act No. 94/1988 Coll., Act No. 188/1988 Coll., Act No. 87/1990 Coll., Act No. 105/1990 Coll., Act No. 116/1990 Coll., Act No. 87/1991 Coll., Act No. 509/1991 Coll., Act No. 264/1992 Coll., Act No. 267/1994 Coll., Act No. 104/1995 Coll., Act No. 118/1995 Coll., Act No. 89/1996 Coll., Act No. 94/1996 Coll., Act No. 227/1997 Coll., Act No. 91/1998 Coll., Act No. 165/1998 Coll., Act No. 159/1999 Coll., Act No. 363/1999 Coll., Act No. 27/2000 Coll., and Act No. 103/2000 Coll., is hereby amended as follows:

Section 40(3) is hereby supplemented with the following sentence: ”Legal procedures performed with the aid of electronic means may be signed electronically, in accordance with special legislation”.

PART THREE. AMENDMENTS TO ACT No. 337/1992 Coll., ON ADMINISTRATION OF TAXES AND FEES ➦

Article 22.-

Act No. 337/1992 Coll., on administrative taxes and fees, as subsequently amended by Act No. 35/1993 Coll., Act No. 157/1993 Coll., Act No. 323/1993 Coll., Act No. 85/1994 Coll., Act No. 255/1994 Coll., Act No. 59/1995 Coll., Act No. 118/1995 Coll., Act No. 323/1996 Coll., Act No. 61/1997 Coll., Act No. 242/1997 Coll., Act No. 91/1998 Coll., Act No. 168/1998 Coll., Act No. 29/2000 Coll., Act No. 159/2000 Coll., and Act No. 218/2000 Coll., is hereby amended as follows:

Sec. 21(2,3) reads:

”(2) Provided that it is so stipulated by this or another Act, taxpayers shall submit their income tax declarations, reports, and remittances to the tax administration authority of competence by venue, using pre-printed forms. Forms issued in electronic form may be signed electronically, in accordance with special legislation.

(3) Other motions concerning tax matters, such as notifications, applications, propositions, objections, appeals, etc. may be submitted in writing; put on record verbally; or submitted in electronic form, signed in accordance with special legislation, or with the aid of transmission technology (telex, fax message, etc.)”

PART FOUR. AMENDMENTS TO THE ADMINISTRATION CODE ➦

Article 23.-

Act No. 71/1967 Coll., on administrative proceedings (the Administration Code), as subsequently amended by Act No. 29/2000 Coll., and is hereby amended as follows:

Section 19(1) reads:

”(1) Motions may be made in writing; put on record verbally; or submitted in electronic form, signed electronically, in accordance with special legislation. Motions may also be made telegraphically; motions containing a proposition concerning a certain matter must be put on record in writing or verbally subsequently within 3 days.”

PART FIVE. AMENDMENTS TO THE RULES OF COURT ➦

Article 24.-

Act No. 99/1993 Coll., the Civil Proceedings Code, as subsequently amended by Act No. 36/1967 Coll., Act No. 158/1969 Coll., Act No. 49/1973 Coll., Act No. 20/1975 Coll., Act No. 133/1982 Coll., Act No. 180/1990 Coll., Act No. 328/1991 Coll., Act No. 519/1991 Coll., Act No. 263/1992 Coll., Act No. 24/1993 Coll., Act No. 171/1993 Coll., Act No. 117/1994 Coll., Act No. 152/1994 Coll., Act No. 216/1994 Coll., Act No. 84/1995 Coll., Act No. 118/1995 Coll., Act No. 160/1995 Coll., Act No. 238/1995 Coll., Act No. 247/1995 Coll., Act No. Finding of the Constitutional court No. 31/1996 Coll., Act No. 142/1996 Coll., Finding of the Constitutional Court No. 269/1996 Coll., Act No. 202/1997 Coll., Act No. 227/1997 Coll., Act No. 15/1998 Coll., Act No. 91/1998 Coll., Act No. 165/1998 Coll., Act No. 326/1999 Coll., Act No. 360/1999 Coll., Finding of the Constitutional Court No. 2/2000 Coll., Act No. 27/2000 Coll., Act No. 30/2000 Coll., Act No. 46/2000 Coll., Act No. 105/2000 Coll., Act No. 130/2000 Coll., Act No. 155/2000 Coll., and Act No. 220/2000 Coll., is hereby amended as follows:

Section 42(1), first sentence reads: ”Motions may be made in writing; put on record verbally; or submitted in electronic form, signed electronically, in accordance with special legislation; or telegraphically or per facsimile.”

PART SIX. AMENDMENTS TO THE PENAL CODE ➦

Article 25.-

Act No. 141/1961 Coll., on penal court proceedings (the Penal Code), as subsequently amended by Act No. 57/1965 Coll., Act No. 58/1969 Coll., Act No. 149/1969 Coll., Act No. 48/1973 Coll., Act No. 29/1978 Coll., Act No. 43/1980 Coll., Act No. 159/1989 Coll., Act No. 178/1990 Coll., Act No. 303/1990 Coll., Act No. 558/1991 Coll., Act No. 25/1993 Coll., Act No. 115/1993 Coll., Act No. 292/1993 Coll., Act No. 154/1994 Coll., Finding of the Constitutional Court No. 214/1994 Coll., Finding of the Constitutional Court No. 8/1995 Coll., Act No. 152/1995 Coll., Act No. 150/1997 Coll., Act No. 209/1997 Coll., Act No. 148/1998 Coll., Act No. 166/1998 Coll., Act No. 191/1999 Coll., Act No. 20/2000 Coll., and Act No. 30/2000 Coll., is hereby amended as follows:

Section 59(1) reads:

(1) Every motion shall be assessed according to its contents, even if incorrectly marked. Motions may be made in writing; put on record verbally; or submitted in electronic form, signed electronically, in accordance with special legislation; or telegraphically or per facsimile.

PART SEVEN. AMENDMENTS TO THE PERSONAL DATA PROTECTION ACT ➦

Article 26.-

Act No. 101/2000 Coll., on protection of personal data and on amendments to certain legislation, is amended as follows:

Section 29 is extended by Paragraph 4, which reads:

"(4) The Office grants and withdraws accreditation to/from entities operating as accredited providers of certification services and supervisors enforcing adherence to obligations stipulated by the Electronic Signature Act."

PART EIGHT. AMENDMENTS TO THE ACT ON ADMINISTRATIVE FEES ➦

Article 27.-

Act No. 368/1992 Coll., on administrative fees, as subsequently amended by Act. No. 10/1993 Coll., Act No. 72/1994 Coll., Act No. 36/1995 Coll., Act No. 118/1995 Coll., Act No. 160/1995 Coll., Act No. 301/1995 Coll., Act No. 151/1997 Coll., Act No. 305/1997 Coll., Act No. 149/1998 Coll., Act No. 157/1998 Coll., Act No. 167/1998 Coll., Act No. 63/1999 Coll., Act No. 166/1999 Coll., Act No. 167/1999 Coll., Act No. 223/1999 Coll., Act No. 326/1999 Coll., Act No. 352/1999 Coll., Act No. 357/1999 Coll., Act No. 360/1999 Coll., Act No. 363/1999 Coll., Act No. 46/2000 Coll., Act No. 62/2000 Coll., Act No. 117/2000 Coll., No. 133/2000 Coll., No. 151/2000 Coll., No. 153/2000 Coll., No. 154/2000 Coll., No. 156/2000 Coll., and No. 158/2000 Coll., is hereby amended as follows:

1. The Annex to the Act (Table of Administrative Fees) is hereby complemented by Part XII that reads:

PART XII. PROCEEDINGS UNDER THE ELECTRONIC SIGNATURE ACT ➦

Article 27

Item 162

a) submission of an application for accreditation by a provider of certification services CZK 100,000.00

b) submission of an application for conformity evaluation of electronic signature instruments CZK 10,000.00

PART XII. PROCEEDINGS UNDER THE ELECTRONIC SIGNATURE ACT ITEM 162 ➦

3. The period (dot) after Part XI is to be omitted.

PART NINE. THE ACT COMES INTO FORCE AND EFFECT ON THE FIRST DAY OF THE THIRD CALENDAR MONTH FOLLOWING PROMULGATION DATE ➦

Klaus, m.p.

Havel, m.p.

Zeman, m.p.

Notes

1) Act No. 40/1964 Coll., the Civil Code, as amended.

2) Sec. 10 of Act No. 40/1964 Coll., as amended by Act No. 509/1991 Coll.

3) Act No. 101/2000 Coll., on personal data protection, and amendments to relevant legislation.

4) Act No. 552/1991 Coll., on state supervision, as amended.

5) Act No. 368/1992 Coll., on administrative fees, as amended.

6) Act No. 85/1996 Coll., on defense law, as amended by Act No. 210/1999 Coll.

Act No. 358/1992 Coll., on notaries and their activities (the Notarial Code), as amended

Act No. 36/1967 Coll., on court experts and interpreters.

7) Sec. 43 of Act No. 71/1967 Coll., on administrative proceedings (the Administration Code).

8) Act No. 337/1992 Coll., on administration and taxes and fees, as amended.

9) Act No. 71/1967 Coll., as amended by Act No. 29/2000 Coll.