REPUBLIC OF SERBIA

ELECTRONIC SIGNATURE LAW

JUGOSLOVENSKI PREGLED
Belgrade, 2009

ELECTRONIC SIGNATURE LAW

Note: This is a true translation of the original Law,
but it is not legally binding.

Original title:
ZAKON O ELEKTRONSKOM POTPISU

Prepared by: *Jugoslovenski pregled* (*Yugoslav Survey*), Dečanska 8/V, Beograd;
Tel/Fax: + 381 11 / 32 33 610, 32 32 295; Tel: 32 41 953, 32 40 291; Po.Box 80 (PAK 106806)
www.pregled-rs.rs • E-mail: info@pregled-rs.rs

CONTENTS

ELECTRONIC SIGNATURE LAW

ELECTRONIC SIGNATURE LAW*

I BASIC PROVISIONS

Article 1

The present Law shall govern the use of the electronic signature in legal transactions and other legal deeds and in the conduct of business, as well as the rights, duties and liabilities associated with the electronic certificates, unless otherwise provided by other laws.

The provisions of the present Law shall also apply to the communications between authorities, communications between authorities and parties and presentation and drawing up of decisions of the authorities in electronic form in the administrative, court and other proceedings before a government agency, if the law governing such proceedings provides for the use of electronic signature.

Article 2

The meaning of some of the terms and expressions used in the present Law shall be as follows:

1) "Electronic document": a document in the electronic form which is used in legal transactions and other legal deeds, as well as in the administrative, judicial and other proceedings before government agencies;

2) "Electronic signature": a set of data in the electronic form which are joined to or logically connected with an electronic document and the purpose of which is to identify the signatory;

3) "Qualified electronic signature": an electronic signature reliably guaranteeing the signatory's identity and integrity of electronic documents and rendering impossible any subsequent denial of liability for their contents, and which meets the requirements provided by the present Law;

4) "Signatory": a person who possesses the electronic signature-forming means and affixes the electronic signature in his/her own name or in the name of a legal entity or individual;

5) "Electronic signature-forming data": unique data, such as codes or private cryptographic keys used by a signatory in affixing the electronic signature;

6) "Electronic signature-forming means": appropriate technical means (software and hardware) used in the formation of an electronic signature, using the electronic signature-forming data;

7) "Qualified electronic signature-forming means": electronic signature forming means, which meet the requirements set by the present Law:

8) "Electronic signature-verifying data": data, such as codes or public cryptographic keys, used in the verification and authentication of electronic signatures;

9) "Electronic signature-verifying means": appropriate technical means (software and hardware) serving for the verification of electronic signatures, using the electronic signature-verifying data;

10) "Qualified electronic signature-verifying means": electronic signature-verifying means which meet the requirements set by the present Law;

11) "Electronic certificate": an electronic document which confirms the connection between the electronic signature-verifying data and the signatory's identity;

12) "Qualified electronic certificate": an electronic certificate which is issued by a certification body for the issuance of electronic certificates and contains the data required by the present Law;

13) "User": a legal entity, sole proprietor, government agency, territorial autonomy agency, local self-government agency or an individual to which/whom the electronic certificate is issued;

---

* Published in the *Republic of Serbia Official Gazette,* No. 135/04 of 21 December 2004.

14) “Certification body”: a legal entity which issues electronic certificates in conformity with the provisions of the present Law.

Article 3

The validity or probative force of an electronic document may not be challenged only because of its being in an electronic form.

Paragraph 1 of this Article shall not apply to the following:

1) Legal transactions with the means of which the title to real estate is transferred to or is serving for the establishment of other real rights in relation to real estate;

2) Statements of the parties to and other participants in the succession hearings, form of legacy, contracts of conveyance and distribution of property during lifetime, contracts of maintenance for life and agreements in connection with inheritance, as well as other agreements in the domain of probate law;

3) Agreements on proprietary relations between spouses;

4) Agreements on the management of property of the persons declared incompetent;

5) Agreements on gifts;

6) Other legal transactions or acts for which special laws or regulations enacted on the basis of them expressly requires the manual affixation of signature in the documents on paper or authentication of the manually affixed signatures.

Article 4

If a law or regulation makes it necessary for a document to be saved, that may also be done electronically, provided that:

1) The electronic document is accessible and available for subsequent use;

2) The electronic document has been saved in the form in which it was formed or received;

3) The electronic document has been saved in a way which makes it possible to identify the time and place of its origin or reception and the person who had formed it;

4) That the methods and procedures used make it possible to establish reliably any alteration made in the electronic document.

The duty to save any document referred to in paragraph 1 of this Article shall not apply to data the sole purpose of which is to allow an electronic document to be received or transmitted (communication data).

Article 5

The persons who are keeping the electronic documents which have been electronically signed shall save the data and means of verifying the electronic signatures for as long as the documents themselves are to be saved.

II ELECTRONIC SIGNATURE AND QUALIFIED ELECTRONIC SIGNATURE

Article 6

An electronic signature may produce legal effect and may be used as evidence in legal proceedings, except when under a special law, only a manually affixed signature can produce legal effect and probative force.

Article 7

A qualified electronic signature shall meet the following requirements:

1) That it is associated with the signatory exclusively;

2) That it identifies the signatory unambiguously;

3) That it comes into being using the means which the signatory can control independently and which are kept under the signatory’s exclusive supervision;

4) That it is directly associated with the data it relates to in a way which unambiguously allows any change made in the original data to be inspected;

5) That it has been formed on the basis of the signatory’s qualified electronic signature;

6) That it can be verified on the basis of the signatory’s qualified electronic certificate.

Article 8

The qualified electronic-signature forming means shall be the means which have to provide for the following:

1) That the qualified electronic-signature forming data may appear only once and that their confidentiality is secured;

2) That it is not possible to obtain from the qualified electronic signature-verifying data the qualified electronic signature-forming data within

a reasonable period of time using the currently available means;

3) That the qualified electronic signature is protected from being forged using the currently available means;

4) That the qualified electronic signature-forming data are reliably protected against unauthorised use.

The qualified electronic signature-forming means may not alter on the occasion of signature forming the data which are being signed or prevent the signatory from seeing such data prior to the qualified electronic signature-forming procedure.

Article 9

The means of verifying a qualified electronic signature shall be such means as will provide for the following:

1) Reliable establishment of the fact that the data used for verification of an electronic signature correspond to the data shown to the person carrying out the verification;

2) Reliable verification of signature and proper presentation of the results of verification;

3) Getting a reliable insight into the contents of the signed data;

4) Reliable verification of the authenticity and validity of the signatory's electronic certificate on the occasion of verification of the electronic signature;

5) Proper presentation of the signatory's identity;

6) Reliable detection of any alteration made in the signed data.

Article 10

In relation to the data in the electronic form, a qualified electronic signature shall produce the same legal effect and probative force as a manually affixed signature and as a manually affixed signature and stamp, in relation to the data in paper form.

Article 11

The ministry responsible for the information society (hereinafter: the competent authority) shall set the technical and technological procedures for the formation of qualified electronic signatures and the criteria to be satisfied by the qualified electronic signature forming means.

III ELECTRONIC CERTIFICATES AND CERTIFICATION BODIES

Article 12

For the purposes of the present Law, an electronic certificate shall mean an electronic confirmation of a connection between the electronic signature-verifying data and the signatory's identity.

Electronic certificates shall be issuable by a certification body.

For the purposes of the present Law, a certification body shall mean a legal entity which renders to other legal entities and individuals electronic certificate issuing services to other legal entities and individuals, as well as other services associated with that business.

Article 13

Certification bodies do not have to possess special electronic certificate-issuing licences.

Article 14

The competent authority shall keep a record of the certification bodies.

Article 15

Any certification body shall notify the competent authority of its commencement with provision of the electronic certificate issuing services at least 15 days beforehand.

Article 16

The competent authority shall enter into records any certification body immediately upon receipt of the notification of its commencement with the provision of services.

The competent authority shall prescribe the contents and modality of keeping records, application forms for entry in records, applications for entering changes and the kind, contents and way of presenting the documents necessary for making entries in records.

Article 17

For the purposes of the present Law, a qualified electronic certificate shall mean an electronic certificate issued by a certification body engaged in the issuance of qualified electronic certificates, which shall contain the following:

1) A note showing that a qualified electronic certificate is involved;

2) Set of data which singly identify the certificate-issuing legal entity;

3) Set of data which singly identify the signatory;

4) Data verifying the electronic signature that correspond to the qualified electronic signature-forming data kept under the signatory's control;

5) Data showing the beginning and end of the electronic certificate's validity;

6) Identity mark of the issued electronic certificate;

7) Qualified electronic signature of the certification body which has issued the qualified electronic certificate;

8) Limitations on the use of certificate, if any.

Article 18

Any certification body shall meet the following requirements for the issuance of qualified electronic certificates:

1) Capacity for reliable provision of the electronic certificate issuing services;

2) Ability to keep the register of users securely and up-to-date, as well as to revoke electronic certificates securely and promptly;

3) Accurate setting of the date and time of the issuance or revocation of electronic certificates;

4) Ability to check the identity and, if necessary, other additional characteristics of the person to whom the certificate is being issued, reliably and in conformity with regulations;

5) Availability of the staff having specialist knowledge, experience and vocational attainment necessary for the provision of the electronic certificate-issuing services, with particular reference to the following: management level capabilities, expertise in the application of the electronic signature technology and appropriate security procedures and secure application of the related administrative and control procedures which are up to recognised standards;

6) Ability to use reliable systems and products which are protected against unauthorised alterations and provide for technical and cryptographic security of the process;

7) Ability to apply measures against electronic certificate forgery and in the cases in which the electronic signature forming data are generated, to guarantee confidentiality of the process of forming such data;

8) Ability to raise the funds required for insurance against such risks and liability for any damage caused by the provision of electronic certificate issuing services;

9) Ability to save all relevant information relating to electronic certificates in a specified period of time, in the original form;

10) Not saving or copying the electronic signature forming data for the persons on behalf of which it is providing such services;

11) Ability to secure systems for the physical protection of appliances, equipment and data and means of protection against unauthorised access;

12) Ability to inform the applicants for qualified electronic certificates as to the exact conditions for the issuance and use of such certificates, including any limitations set on their use, as well as the procedures for the settlement of disputes. Such information, which may be conveyed by electronic means, shall be written and prepared in a coherent form in the Serbian language. Appropriate parts of such information shall be accessible on request to third parties which are using electronic certificates;

13) Ability to use a reliable system of electronic certificate management in the form that allows them to be checked in order to ensure the following:

(a) That only authorised persons may make entries and changes;

(b) That the authenticity of the information contained in the certificates can be verified;

(c) That electronic certificates are made accessible to the public for searching purposes only in the cases approved by the certificate owners;

(d) That any technical alteration that could be disruptive to the security requirements is made known to the certification body.

The competent authority shall prescribe in greater detail the conditions for and way of checking whether the requirements referred to in paragraph 1 of this Article have been satisfied.

Article 19

The competent authority shall keep the Register of Certification Bodies for the Issuance of Qualified Electronic Certificates in the Republic of Serbia (hereinafter: the Register).

The competent authority shall prescribe the contents and way of keeping the Register, way for applying for entry in the Register, documents to be attached to the application, application form and way of publishing the data entered in the Register.

Article 20

If a certification body meets the requirements referred to in Article 18 of the present Law, the competent authority shall render a decision allowing it be entered in the Register.

The decision shall be rendered at the request of the certification body concerned with 30 days from the filing date of a proper application for it.

The decision shall include the number under which the certification body concerned has been entered in the Register and the date of entry in the Register.

Any certification body may begin to provide the qualified electronic certificate issuing services as of the date of its entry in the Register.

The certification bodies which have been entered in the Register may state that fact in the qualified certificates issued by them.

Article 21

Qualified electronic certificates may also be issued by government agencies, in conformity with special regulations.

Article 22

The Register and records of certification bodies shall be accessible to the public.

IV RIGHTS, DUTIES AND LIABILITIES OF USERS AND CERTIFICATION BODIES

Article 23

An electronic certificate may be issued to a user on its own request on the basis of a special contract.

A user may choose the certification body by itself, except in the cases determined by special regulations.

A user may use the certification services of one or several certification bodies.

Article 24

A qualified electronic certificate may be issued to any person on its own request, on the basis of its identity which has been established beyond any doubt and other data relating to the applicant.

Article 25

Any user shall keep the electronic signature-forming means and data safe from unauthorised access and use, and use them in conformity with the provisions of the present Law.

Article 26

Any user shall present to the certification body all of the required data and information on the changes that affect or could affect the accuracy of establishing the signatory's identity promptly, though no later than within seven days from the occurrence of change.

Any user shall file promptly a request for the revocation of its certificate in the event of loss of or damage to the electronic signature/forming means or data.

Article 27

Any user shall be liable for any irregularity resulting from non-fulfilment of the obligations referred to in Articles 25 and 26 of the present Law.

Any user may be relieved of liability in the cases in which it is possible to prove that the injured person did not take steps towards verifying the electronic signature and electronic certificate or did so incorrectly.

Article 28

The duties of any certification body engaged in the issuing of qualified electronic certificates shall be as follows:

1) Making sure that each qualified electronic certificate issued contains all of the data referred to in Article19 of the present Law;

2) Thorough checking on the identity of the user to whom the certification service is being rendered;

3) Seeing to the accuracy and completeness of the data entered in the record of issued certificates;

4) Entering in each certificate the basic data relating to its own identity;

5) Making it possible for any interested person to inspect the certification body's identification data and inspect the permit for issuing qualified electronic certificates;

6) Keeping up-to-date, accurate and secured records of issued electronic certificates, which must be accessible to the public, except in the cases in which the certificate owner expressly requests that its data are not to be accessible to the public;

7) Keeping an accurate and secure record of invalid electronic certificates;

8) Making sure that the exact date and time (hour and minute) of the issuance or revocation of electronic certificates are visible in the records of issued electronic certificates;

9) Acting in compliance with the provisions of laws and regulations governing the safeguarding of personal data.

Article 29

Prior to concluding a contract referred to in Article 23, paragraph 1, of the present Law, any certification body engaged in the issuing of qualified electronic certificates shall notify the applicant for a qualified electronic certificate of all important circumstances pertaining to its use.

The notification referred to in paragraph 1 of this Article shall include the following:

1) An excerpt from standing regulations, internal rules and other conditions relating to the use of electronic certificates;

2) Any limitations on the use of electronic certificates;

3) Legal remedies available in the event of disputes;

4) Steps to be taken by the users of certificates and the necessary equipment for secure electronic signing and verification of electronic signatures.

Article 30

Any certification body shall discontinue the provision of certification services and/or revoke the issued qualified electronic certificates in the following cases:

1) If the revocation of a certificate is requested by the owner of that certificate or his/her proxy;

2) If the owner of a certificate is declared incompetent or has ceased to exist or if the circumstances affecting the validity of the certificate have changed substantially;

3) If it establishes that a datum in the certificate is wrong or that the certificate was issued on the basis of wrong data;

4) If it establishes that the electronic signature/verifying data or the certification body's information system are endangered in a way that affects the certificate's security and reliability;

5) If it establishes that the electronic signature data or the information system of the certificate owner is endangered in a way that affects the reliability and security of the electronic signature forming;

6) If it ceases to operate or is banned from operating and the validity of the issued certificates is still running.

Any certification body shall keep up-to-date records of all revoked electronic certificates.

Any certification body shall notify the user concerned of the revocation of an electronic certificate within 24 hours from receipt of information or onset of the circumstances owing to which that electronic certificate is being revoked.

Article 31

Any certification body engaged in the issuing of qualified electronic certificates shall save all documents relating to the issued and revoked electronic certificates as evidence and means of verification in judicial, administrative and other proceedings, for at least ten years from expiration of the validity of qualified electronic certificates.

The data referred to in paragraph 1 of this Article may be saved in the electronic form.

Article 32

Any certification body shall notify each user and the competent authority of the termination of a contract because of the need for or intention to withdraw from business, at least three months before the onset of such circumstances.

Any certification body shall arrange with another certification body for the continued provision of certification services to the users to which it had issued certificates and should that not be possible, it shall revoke all of the issued certificates and promptly notify the competent authority accordingly.

Any certification body which is ceasing to provide certification services shall hand over all documents relating to the provision of certification services to another certification body to which it is assigning the provision of certification services or to the competent authority, if another certification body is not available.

The competent authority shall revoke promptly all of certificates issued by a certification body that

has stopped engaging in certification for any reason and has not arranged for certification to be done by another certification body and revoked the issued certificates, at the expense of the certification body concerned.

Article 33

The competent authority shall prescribe the lowest insurance against risk and liability for any damage resulting from the provision of electronic certificate issuing services.

Article 34

Any certification body which is issuing qualified electronic certificates or guarantees the qualified electronic certificates of some other certification body shall be liable for any damage done to a person who has relied on such certificate in the following cases:

1) If the information included in a qualified electronic certificate was not correct at the time of its issuance;

2) If the certificate does not include all of the elements prescribed for a qualified electronic certificate;

3) If it has not checked at the moment of issuance of the certificate whether the signatory is in possession of the electronic signature forming data which correspond to the electronic signature verification data which were stated or identified in the certificate;

4) If it fails to make sure that the electronic signature forming and verification data can be used complementarily, in the cases in which such data are generated by the certification body;

5) If it fails to revoke a certificate in compliance with the provisions of Article 30 of the present Law;

6) If a certificate does not contain the information on any limitations relating to the use of certificate, which are included in the contract made with the user.

No certification body shall be liable for the damage referred to in paragraph 1 of this Article, if it proves that it has acted in accordance with law and its general and internal rules of operation.

No certification body shall be liable for any damage resulting from the use of a certificate beyond the scope of limitations, if such limitations are clearly stated in the certificate.

Article 35

The electronic certificates issued by any foreign certification body shall enjoy the same treatment as domestic electronic certificates.

The qualified electronic certificates issued by foreign certification bodies shall enjoy the same treatment as the domestic ones in the following cases:

1) If the foreign verification body concerned has obtained the competent authority's permit pursuant to Articles 18 and 20 of the present Law, or

2) If they originate from a country with which a bilateral agreement has been concluded on the mutual recognition of qualified electronic certificates.

V SUPERVISION

Article 36

The competent authority shall exercise inspective supervision over the enforcement of the present Law and operation of the certification bodies.

The authorities duly designated by the laws and regulations governing the safeguarding of personal data shall supervise the operation of certification bodies in the collection, use and safeguarding of the personal data of users.

Article 37

In the scope of inspective supervision over the registered and recorded certification bodies, the Ministry shall do as follows:

1) Establish whether the requirements set by the present Law and the regulations enacted in support of enforcement of the present Law have been met;

2) Check whether the prescribed procedures and organisational and technical measures are being properly applied and on the application of internal rules associated with the requirements set by the present Law and the regulations enacted in support of the enforcement of the present Law;

3) Check on the issuing, keeping and revocation of electronic certificates;

4) See whether the certification bodies are providing other services lawfully.

Article 38

In exercising the inspective supervision over the operation of certification bodies, the duly authorised competent authority's officers shall have the right and duty to do the following:

1) Examine the deeds and all documents associated with such activity;

2) Inspect their business premises, information system, computer network, technical documents and the security measures applied;

3) Examine all files for the purpose of obtaining evidence or establishing any irregularities accurately.

The duly authorised officer of the competent authority shall keep as official secret all of the data relating to certificates and personal data on the users of certificates.

Article 39

Any duly authorised officer of the competent authority may do the following:

1) Prohibit the use of improper procedures and infrastructure and set a time limit within which the certification body concerned has to secure the proper procedures and infrastructure;

2) Prohibit a certification body from operating pending the putting of the procedures and infrastructure in good order;

3) Issue an order temporarily revoking any or all certificates issued by the certification body concerned in the event of reasonable doubt that improper procedure or forgery is involved.

In the case of a temporary prohibition from operation, the certificates issued prior to the date of onset of the reasons for prohibition, shall remain valid.

Article 40

Should a certification body engaged in the issuing of qualified electronic certificates stop meeting the requirements determined by the present Law, the competent authority shall render a decision deleting it from the register of certification bodies engaged in the issuing of qualified electronic certificates.

The decision referred to in paragraph 1 of this Article shall be final and administrative action may be filed against it.

Article 41

For the purpose of exercising supervision, any certification body shall allow the duly authorised officers of the competent authority access to its business premises and make it possible for the latter to inspect its business data and its books and access to the register of users and the computing equipment and appliances used.

VI PENAL PROVISIONS

Article 42

Any user which is a legal entity shall be fined 100,000 to 400,000 Dinars for breach of regulations in the following cases:

1) If it is not keeping the electronic signature-forming means and data safe from unauthorised access and use and if it is not using them in conformity with the provisions of the present Law (Article 25);

2) If it does not present to the certification body within the prescribed term the necessary data and information on the changes that affect or could affect the accuracy of establishing the signatory's identity (Article 26, paragraph 1);

3) If it does not present to the certification body promptly the request for the revocation of an electronic certificate (Article 26, paragraph 2).

Any user who is a sole proprietor shall be fined 100,000 to 200,000 Dinars for any breach of regulations referred to in paragraph 1 of this Article.

The responsible person in a legal entity, government agency, territorial autonomy agency and local self-government agency shall be fined 12,000 to 20,000 Dinars for any breach of regulations referred to in paragraph 1 of this Article.

Any user who is an individual shall be fined 12,000 to 20,000 dinars for any breach of regulations referred to in paragraph 1 of this Article.

Article 43

Any certification body shall be fined 200,000 to 400,000 Dinars for breach of regulations in the following cases:

1) If it fails to notify the competent authority that it has started to provide electronic certificate issuing services (Article 15);

2) If it issues a qualified electronic certificate which does not contain the necessary data (Article 17);

3) If it keeps and copies the electronic signature forming data for the persons in whose name it provides such services (Article 18, item 10);

4) If it fails to notify the user to whom it is issuing an electronic certificate of the exact requirements for the issuance and use of that electronic certificate (Article 18, item 12);

5) If it fails to perform the duties referred to in Article 28;

6) If it does not stop providing the certification services or does not revoke the issued qualified electronic certificates in the prescribed cases (Article 30, paragraph 1);

7) If it does not keep up to date a record of all revoked electronic certificates (Article 30, paragraph 2);

8) If it fails to notify a user of the revocation of an electronic certificate within the set term (Article 30, paragraph 3);

9) If it does not keep the complete documents relating to issued and revoked qualified electronic certificates in the prescribed duration (Article 31, paragraph 1);

10) If it fails to notify timely the users to whom it has issued electronic certificates and the competent authority of the circumstances which could cause it to stop providing the certification services (Article 32, paragraph 1);

11) If it does not make it possible for duly authorised officers of the competent authority to enter its premises, inspect its business data and business books and get access to the register of users, computer equipment and appliances (Article 38).

The responsible person in the certification body concerned shall be fined 15,000 to 20,000 Dinars for any breach of regulations referred to in paragraph 1 of this Article.

Article 44

Any legal entity shall be fined 200,000 to 400,000 Dinars for breach of regulations in the event of its failure to keep the electronic signature verifying data and means for as long as it is necessary to keep the electronic documents themselves (Article 5).

Any sole proprietor shall also be fined 100,000 to 200,000 Dinars for a breach of regulations referred to in paragraph 1 of this Article.

The responsible person in a legal entity, government agency, territorial autonomy agency and local self-government agency shall be fined 12,000 to 20,000 Dinars for the breach of regulations referred to in paragraph 1 of this Article.

VII TRANSITIONAL AND CONCLUDING PROVISIONS

Article 45

The competent authority shall issue the regulations for the enforcement of the present Law within three months from the effective date of the present Law.

Article 46

The present Law shall come into force on the eighth day upon its publication in the Official Gazette of the Republic of Serbia.