

**LAW No. 04/L-094  
ON THE INFORMATION SOCIETY SERVICES**

**Assembly of Republic of Kosovo,**

Based on Article 65 (1) of the Constitution of the Republic of Kosovo;

Approves:

**LAW ON THE INFORMATION SOCIETY SERVICES**

**CHAPTER I  
GENERAL PROVISIONS**

**Article 1  
Purpose and Scope**

1. This Law shall make electronic documentation legally equivalent to its traditional counterpart in paper format, in order to facilitate electronic services including, but not limited to, consumer shopping and sales over the internet (eCommerce), electronic banking and financial services (ePayment), government provision of services (eGovernment) and electronic purchasing by enterprises (eProcurement) and applies where electronic signatures are used.

2. The purpose of this law is to establish convenient possibilities and circumstances for development of electronic trade, use of electronic transactions and electronic signature by the Government, businesses and citizens too. The purpose of this law is, also, to reduce the potential problems and abuses during the electronic transactions as well as addressing safety of information system.

3. This Law applies to any kind of information in the form of a data message, except in the following cases:

- 3.1. contracts that create or transfer rights in real estate, except for rental rights;
- 3.2. contracts requiring by law the involvement of courts, public authorities or professions exercising public authority;
- 3.3. contracts of surety ship granted and on collateral securities furnished by persons acting for purposes outside their trade, business or profession;
- 3.4. contracts governed by family law or by the law of succession.

**Article 2  
Definitions**

1. Terms used in this Law shall have the following meanings:

- 1.1. **Voluntary accreditation** - any permission, setting out rights and obligations specific to the provision of signature certification services, to be granted upon request by the certification service provider concerned, by the public or private body charged with the elaboration of, and supervision of compliance with such rights and obligations, where the

certification service provider is not entitled to exercise rights stemming from the permission until it has received the decision by the body.

**1.2. Telecommunications Regulatory Authority** (“TRA”) - the independent regulatory body established by this Law to regulate and foster the development of the telecommunications sector in Kosovo.

**1.3. Originator of a data message** - a person by whom or on whose behalf, the data message purports to have been sent or generated prior to storage, if any, but it does not include a person acting as an intermediary with respect to that data message.

**1.4. Certificate** - an electronic attestation, which links the signature verification data to a person and confirms the identity of that person.

**1.5. Qualified certificate** - a certificate issued by a certification service provider and that contains:

- 1.5.1. an indication that the certificate is issued as a qualified certificate;
- 1.5.2. the identification of the certification-service-provider and the State in which it is established;
- 1.5.3. the name of the signatory or a pseudonym, which shall be identified as such;
- 1.5.4. provision for a specific attribute of the signatory to be included if relevant, depending on the purpose for which the certificate is intended;
- 1.5.5. signature-verification data which correspond to signature-creation data under the control of the signatory;
- 1.5.6. an indication of the beginning and end of the period of validity of the certificate;
- 1.5.7. the identity code of the certificate;
- 1.5.8. the advanced electronic signature of the certification-service-provider issuer;
- 1.5.9. limitations on the scope of use of the certificate, if applicable; and
- 1.5.10. limits on the value of transactions for which the certificate can be used, if applicable.

**1.6. Commercial** - all matters arising from all relationships of a commercial nature, whether contractual or not. Relationships of a commercial nature include, but are not limited to, the following transactions:

- 1.6.1 any trade transaction for the supply or exchange of goods or services;
- 1.6.2. distribution agreements;
- 1.6.3. commercial representation or agency;
- 1.6.4. factoring;

1.6.5. leasing;

1.6.6. construction of works;

1.6.7. consulting;

1.6.8. engineering;

1.6.9. licensing;

1.6.10. investment;

1.6.11. financing;

1.6.12. banking;

1.6.13. insurance;

1.6.14. exploitation agreement or concession;

1.6.15. joint venture and other forms of industrial or business cooperation;

1.6.16. carriage of goods or passengers by air, sea, rail or road.

1.7. **Computer** - any device or group of inter-connected or related devices, one or more of which, pursuant to a program, performs automatic processing of computer data.

1.8. **Communication** - any information exchanged or conveyed between a finite number of parties by means of a publicly available electronic communications service. This does not include any information conveyed as part of a broadcasting service to the public over an electronic communications network except to the extent that the information can be related to the identifiable subscriber or user receiving the information.

1.9. **Consumer** - a registered user and/or the one who has signed any certain relation with service provider.

1.10. **Electronic contract** - a contract concluded wholly or partly by electronic communications or in an electronic form.

1.11. **Controller** - any natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data.

1.12. **Issuer** - any public, banking or credit institution issuing a payment card for electronic use, or for any production or service.

1.13. **Addressee of a data message** - a person who is intended by the originator to receive the data message, but does not include a person acting as an intermediary with respect to that data message.

1.14. **Data message** - information generated, sent, received or stored by electronic, optical or similar means including, but not limited to, electronic data interchange (EDI), electronic mail, telegram, telex or telecopy.

1.15. **Electronic** - the service is sent initially and received at its destination by means of electronic equipment for the processing (including digital compression) and storage of

data, and entirely transmitted, conveyed and received by wire, by radio, by optical means or by other electromagnetic means;

1.16. **Minister** - Minister responsible for Information Society Services;

1.17. **Ministry** - Ministry responsible for Information Society Services;

1.18. **Electronic signature** - data in electronic form in, affixed to, incorporated in or logically associated with, a data message, which may be used to identify the signatory in relation to the data message;

1.19. **Advanced electronic signature** - an electronic signature which meets the following requirements:

1.19.1. it is uniquely linked to the signatory;

1.19.2. it is capable of identifying the signatory;

1.19.3. it is created using means that the signatory can maintain under his sole control; and

1.19.4. it is linked to the data to which it relates in such a manner that any subsequent change of the data is detectable.

1.20. **Signatory** - a person that holds signature creation data and acts either on its own behalf or on behalf of the person it represents;

1.21. **Intermediary with respect to a particular data message** - a person who, on behalf of another person, sends, receives or stores that data message or provides other services with respect to that data message.

1.22. **Interoperability** - a state of affairs whereby cards issued in Kosovo or any Member State of the EU and/or belonging to a given card system can be used in other Member States of the EU and/or in the networks installed by other systems. This requires that the cards and readers used in the various systems must be technologically compatible and that systems must be opened up by means of reciprocity agreements.

1.23. **Certification service provider** - a person that issues certificates or provides other services related to electronic signatures pursuant to the Law.

1.24. **Relying party** - a person that may act on the basis of a certificate or an electronic signature.

1.25. **Electronic payment** - any direct or deferred payment transaction carried out by electronic means, except payments by cheque with a bank card guarantee and payments by card using mechanical processes (invoice slips);

1.26. **Signature-creation device** - configured software or hardware used to implement the signature-creation data;

1.27. **Secure-signature-creation device** - a signature-creation device which, by appropriate technical and procedural means, meets the following requirements:

1.27.1. it ensures that the signature-creation-data used for signature generation can practically occur only once, and that their secrecy is reasonably assured;

1.27.2. It ensures that the signature-creation-data used for signature generation cannot, with the level of reasonable assurance, be derived and that the signature is protected against forgery using currently available technology;

1.27.3. it ensures that the signature-creation-data used for signature generation can be reliably protected by the legitimate signatory against the use of others;

1.27.4. secure signature-creation devices does not alter the data to be signed or prevent such data from being presented to the signatory prior to the signature process.

1.28. **Authorized person** - any natural or legal person who has the right, by contract or by law, or the lawful permission, to use, manage, control, test, conduct legitimate scientific research or otherwise operate an information system and who is acting in accordance with that right or permission.

1.29. **Consent** - by a user or subscriber corresponds to the data subject's consent according to the EU legislation.

1.30. **Subject's consent** - any freely given specific and informed indicator of his wishes by which the data subject signifies his agreement to personal data relating to him being processed.

1.31. **Data interception by technical aspect** - non-public transmissions of computer data to, from or within an Information System.

1.32. **Electronic mail** - any text, voice, sound or image message sent over a public communications network which can be stored in the network or in the recipient's terminal equipment until it is collected by the recipient.

1.33. **Processing with relation to personal data** - any operation or set of operations which is performed upon personal data: personal data, whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction.

1.34. **Electronic communications network** - transmission systems and, where applicable, switching or routing equipment and other resources which permit the conveyance of signals by wire, by radio, by optical or by other electromagnetic means, including satellite networks, fixed (circuit- and packet-switched, including Internet) and mobile terrestrial networks, electricity cable systems, to the extent that they are used for the purpose of transmitting signals, networks used for radio and television broadcasting, and cable TV networks, irrespective of the type of information conveyed.

1.35. **Information system** - a system for generating, sending, receiving, storing or otherwise processing data messages.

1.36. **Information Society Services** - any service which is provided at a distance, by electronic means and at the individual request of a recipient of the service, whether such service is provided for consideration or not, and for the purposes of this definition:

1.36.1. **at a distance** means that the service is provided without the parties being simultaneously present;

1.36.2. **by electronic devices** means that the service is sent initially and received at its destination by means of electronic equipment for the processing (including

digital compression) and storage of data, and entirely transmitted, conveyed and received by wire, by radio, by optical means or by other electromagnetic means;

1.36.3.**at the individual request of a recipient of services** means that the service is provided through the transmission of data on individual request.

1.37.**User** - any natural person who for using a publicly available electronic communications service, has no need or is not obliged to make any prior registration.

1.38.**Electronic Data Interchange (EDI)** - the electronic transfer from computer to computer of information using an agreed standard to structure the information.

1.39. **Signature verification data** - data, such as codes, or public cryptographic keys, which are used for the purpose of verifying an electronic signature.

1.40.**Trader with respect to electronic payments** - a natural or legal person providing goods or services.

1.41.**Cardholder** - a credit or debit cardholder, with respect to electronic payments.

1.42.**Inertia sale** – illegal practices of delivering un-requested goods, with an invoice for the good's price.

### **Article 3 Variation by Agreement**

1. As between parties involved in generating, sending, receiving, storing or otherwise processing data messages, and except as otherwise provided, the provisions of Chapter II may be varied by agreement.
2. Paragraph 1. of this Article does not affect any right that may exist to modify by agreement any rule of law referred to in Chapter II.

## **CHAPTER II APPLICATION OF LEGAL REQUIREMENTS TO DATA MESSAGES**

### **Article 4 Legal Recognition of Data Messages**

Information shall not be denied the legal effect, validity or enforceability, solely that it is in the form of a data message, or that it is not contained in the data message but it is merely referred to in the data message that has created such legal effect.

### **Article 5 Writing**

1. If under any law in Kosovo a person is required or permitted to give information in writing, that requirement shall be deemed to have been satisfied by the person if the person gives the information by means of a data message, provided that:

1.1. at the time the information was given, it was reasonable to expect that the information would be readily accessible so as to be usable for subsequent reference; and

1.2. if the information is required to be given to a person, or to another person on his behalf, and the first mentioned person requires that the information be given in

accordance with particular information technology requirements, by means of a particular kind of data message, that person's requirements have been met;

1.3. if the information is required to be given to a person, then the person to whom the information is required or permitted to be given, consents to the information being given by means of a data message; and

1.4. if the information is required to be given to a person, or to another person on his behalf, and the first mentioned person requires that a particular action be taken by way of verifying the receipt of the information, that person's requirement has been met.

2. For the purposes of this Article, giving information includes, but is not limited to:

2.1. making an application;

2.2. making or lodging a claim;

2.3. giving sending or serving a notification;

2.4. lodging a return;

2.5. making a request;

2.6. making a declaration;

2.7. lodging or issuing a certificate;

2.8. lodging an objection; and

2.9. making a statement.

3. For purposes of this Article, a requirement or permission in relation to a person to give information shall extend to and shall be equally applicable to the requirement or information which is stated to be sent, filed, submitted, served or otherwise transmitted and includes similar or cognate expressions thereof.

## **Article 6 Signature**

1. If under any law in Kosovo the signature of a person is required, such requirement is considered as fulfilled if such signature is an electronic signature and such signature shall not deny the legal effectiveness on the grounds that it is:

1.1. in electronic form; or

1.2. not based upon a qualified certificate; or

1.3. not based upon a qualified certificate issued by an accredited certification service provider; or

1.4. not created by a secure signature creation device.

2. Provided that if the electronic signature is in the form of an advanced electronic signature, which is based on a qualified certificate and is created by a secure signature creation device, it shall for all intents and purposes of the law be presumed to be the signature of the signatory.

3. Paragraph 1. of this Article applies whether the requirement therein is in the form of an obligation or whether the law simply provides consequences for the absence of a signature.

### **Article 7 Original**

1. Unless otherwise provided in this Law or by any other law, a person is required to produce or retain a document in its original form, that requirement is met by a data message if:

1.1. there exists a reliable assurance as to the integrity of the document from the time when it was first generated in its final form, as a data message or otherwise;

1.2. at the time the data message was sent, it was reasonable to expect that the information contained in the electronic form of the document would be readily accessible so as to be useable for subsequent reference;

1.3. if the document is required to be produced to a person, or to another person on his behalf, and the first mentioned person requires that the document be given in accordance with particular information technology requirements, by means of a particular kind of data message, that person's requirements have been met; and

1.4. if the document is required to be produced to a person, then the person to whom the information is required or permitted to be given, consents to the information being given by means of a data message; and

1.5. if the document is required to be given to a person, or to another person on his behalf, and the first mentioned person requires that a particular action be taken by way of verifying the receipt of the document, that person's requirement has been met.

2. Paragraph 1. of this Article applies whether the requirement therein is in the form of an obligation or whether the law provides consequences for the information not being presented or retained in its original form.

3. For the purposes of this Article, the integrity of information contained in a document is only maintained in the information remains complete and unaltered, save for:

3.1. the addition of any endorsement; or

3.2. any changes not being change to the information, which is necessary in the normal course of communication, storage or display.

### **Article 8 Retention of Data Messages**

1. If under any law in Kosovo, a person is required to record information in writing, that requirement is deemed to have been satisfied if the person records the information in electronic form provided that such information in electronic form is readily accessible so as to be useable for subsequent reference and it complies with such regulations as may be prescribed.

2. If under any law in Kosovo, a person is required to retain, for a particular period, a document that is in the form of a paper or of any other substance or material, that requirement is deemed to have been satisfied if the person retains an electronic form of the document throughout that period, provided that if:

2.1. having regard to all the relevant circumstances at the time of the generation of the electronic form of the document, the method of generating the electronic form of the

document, provided a reliable means of assuring the maintenance of the integrity of the information contained in that document; and

2.2.at the time of the generation of the electronic form of the document, it was reasonable to expect that the information contained in the electronic form of the document would be readily accessible so as to be useable for subsequent reference; and

2.3.it complies with such regulations as may be prescribed.

3. For the purpose of paragraph 2. of this Article, the integrity of information contained in a document is only maintained if the information has remained complete and unaltered, save for:

3.1. the addition of any endorsement; or

3.2. any change not being a change to the information, which is necessary in the normal course of communication, storage or display.

4. If under any law in Kosovo, a person is required to retain, for a particular period, information that was the subject of an electronic communication, that requirement is deemed to have been satisfied if that person retains, or causes another person to retain, in electronic form, that :

4.1 at the time of commencement of the retention of the information, it was reasonable to expect that the information would be readily accessible so as to be useable for subsequent reference; and

4.2 having regard to all the relevant circumstances, at the time of commencement of the retention of the information, the method of retaining the information in electronic form provided a reliable means of assuring the maintenance of the integrity of the information contained in the electronic communication; and

4.3 throughout that period that person also retains, or causes another person to retain, in electronic form, such additional information obtained as is sufficient to enable the identification of the following:

4.3.1. the origin of the electronic communication;

4.3.2. the destination of the electronic communication;

4.3.3. the time when the electronic communication was sent;

4.3.4. the time when the electronic communication was received; and

4.3.5. at the time of commencement of the retention of the additional information specified in this sub-paragraph it was reasonable to expect that the additional information would be readily accessible so as to be useable for subsequent reference; and

4.3.6. it complies with such regulations as may be prescribed.

5. For the purposes of paragraph 4. of this Article, the integrity of the information which is the subject of an electronic communication is only maintained if the information remains complete and unaltered, save for:

5.1 the addition of any endorsement; or

5.2 any change not being a change to the information, which arises in the normal course of communication, storage or display.

**Article 9**  
**Admissibility and Evidential Weight of Data Messages**

1. In any legal proceedings, shall not be applicable rules of evidence that deny the admissibility of a data message in evidence:

1.1. only because it is a data message; or

1.2. because it is not in original form, if it is the best evidence that can be found from the person adducing it.

2. Information in the form of a data message shall be assessed as any other evidence. In assessing the evidential weight of a data message, a special attention should be paid to the reliability of the manner in which the data message was created, stored or communicated, the manner in which the integrity of the information was maintained, the manner in which its sender/creator was identified and any other relevant factor.

**Article 10**  
**Acceptance and effectiveness**

1. The Minister may, where necessary in cooperation with other Ministers whom it may concern, make regulations to provide for any matter related to Information Society services in order to give fuller effect to the provisions of this Law and in particular, but without prejudice to the generality of this Law such regulations may provide for:

1.1 any derogation or restriction in relation to any cross-border transaction here this is necessary for one of the following reasons:

1.1.1. public policy, in particular the protection of minors, or the fight against any incitement to hatred on the grounds of race, sex, religion, ethnicity, religion, political opinion or nationality;

1.1.2. protection of public health;

1.1.3. public security;

1.1.4. consumer protection;

1.2. identify:

1.2.1. transactions

1.2.2. requirements or permissions to give information in writing;

1.2.3. requirements or permissions to produce documents;

1.2.4. requirements to retain information, documents and communications;

1.2.5 signatures;

1.3. that may be exempt from any provision of this Law;

- 1.4. additional requirements for the use of signatures in data messages in the public sector;
  - 1.5. the consent of public bodies or persons acting on behalf of public bodies to information being given by means of a data message;
  - 1.6. the compliance with any international obligation entered into by Government in relation to any aspect of information society services regulated by or under this Law;
2. The Minister shall establish a computer emergency response center with the aim to deal with threats to public electronic communication systems.

### **CHAPTER III COMMUNICATION OF DATA MESSAGES**

#### **Article 11 Validity of Electronic Contract**

1. An electronic contract shall not be denied legal effect, validity or enforceability solely on the grounds that it is wholly or partly in electronic form or has been entered into wholly or partly by way of electronic communications or otherwise.
2. For the purposes of any law relating to contracts, an offer, an acceptance of an offer and any related communication, including any subsequent amendment, cancellation or revocation of the offer, the acceptance of the contract may, unless otherwise agreed by the contracting parties, be communicated by means of electronic communications.

#### **Article 12 Attribution of Data Messages**

1. A data message is that of the originator if it was sent by the originator itself.
2. As between the originator and the addressee, a data message is deemed to be that of the originator if it was sent:
  - 2.1. by a person who had the authority to act on behalf of the originator in respect of that data message; or
  - 2.2. by an information system programmed by, or on behalf of, the originator to operate automatically.
3. As between the originator and the addressee, an addressee is entitled to regard a data message as being that of the originator, and to act on that assumption, if:
  - 3.1. in order to ascertain whether the data message was that of the originator, the addressee properly applied a procedure previously agreed to by the originator for that purpose; or
  - 3.2. the data message as received by the addressee resulted from the actions of a person whose relationship with the originator or with any agent of the originator enabled that person to gain access to a method used by the originator to identify data messages as its own.
4. Paragraph 3. of this Article does not apply:

- 4.1. as of the time when the addressee has both received notice from the originator that the data message is not that of the originator, and had reasonable time to act accordingly; or
  - 4.2. in a case within subparagraph 3.2. paragraph 3. of this Article, at any time when the addressee knew or should have known, had it exercised reasonable care or used any agreed procedure, that the data message was not that of the originator.
5. The addressee is entitled to deem as acceptable the data message as the originator intended to send and to act on that assumption, if the data message is of the originator or deemed to be as of originator.
6. The addressee is not so entitled according to paragraph 5. of this Article, when it knew or should have known that the transmission resulted in any error in the data message as received.
7. The addressee is entitled to regard each data message received as a separate data message and to act on that assumption, except to the extent that it duplicates another data message and the addressee knew or should have known, had it exercised reasonable care or used any agreed procedure, that the data message was a duplicate.

### **Article 13** **Receipt of acknowledgement**

1. Where the originator has not agreed with the addressee that the acknowledgement be given in a particular form or by a particular method, an acknowledgement may be given by:
  - 1.1. any communication by the addressee, automated or otherwise, or
  - 1.2. any conduct of the addressee, sufficient to indicate to the originator that the data message has been received.
2. Where the originator has stated that the data message is conditional on receipt of the acknowledgement, the data message is treated as though it has never been sent, until the acknowledgement is received.
3. Where the originator has not stated that the data message is conditional on receipt of the acknowledgement, and the acknowledgement has not been received by the originator within the time specified or agreed or, if no time has been specified or agreed, within a reasonable time, the originator:
  - 3.1. may give notice to the addressee stating that no acknowledgement has been received and specifying a reasonable time by which the acknowledgement must be received; and
  - 3.2. if the received is not acknowledgement within the time specified in subparagraph 3.1 of this paragraph, may, upon notice to the addressee, treat the data message as though it had never been sent, or exercise any other rights it may have.
4. Paragraphs 1. to 2. of this Article apply where, on or before sending a data message, or by means of that data message, the originator has requested or has agreed with the addressee that receipt of the data message be acknowledged.
5. Where the originator receives the addressee's acknowledgement of receipt, it is presumed that the related data message was received by the addressee. That presumption does not imply that the data message corresponds to the message received.

6. Where the received acknowledgement states that the related data message met technical requirements, either agreed upon or set forth in applicable standards, it is presumed that those requirements have been met.

7. Except in so far as it relates to the sending or receipt of the data message, this Article is not intended to deal with the legal consequences that may flow either from that data message or from the receipt of its acknowledgement.

#### **Article 14** **Time and Place of Dispatch and Receipt of Data Messages**

1. Unless otherwise agreed between the originator and the addressee, the dispatch of a data message occurs when it enters an information system outside the control of the originator or of the person who sent the data message on behalf of the originator.

2. Unless otherwise agreed between the originator and the addressee, the time of receipt of a data message is determined as follows:

2.1. if the addressee has designated an information system for the purpose of receiving data messages, receipt occurs:

2.1.1. at the time when the data message enters the designated information system; or

2.1.2. if the data message is sent to an information system of the addressee that is not the designated information system, at the time when the data message is retrieved by the addressee;

2.1.3. if the addressee has not designated an information system, receipt occurs when the data message enters an information system of the addressee.

3. Paragraph 2. of this Article applies notwithstanding that the place where the information system is located may be different from the place where the data message is deemed to be received under paragraph 4. of this Article.

4. Unless otherwise agreed between the originator and the addressee, a data message is deemed to be dispatched at the place where the originator has its place of business, and is deemed to be received at the place where the addressee has its place of business. For the purposes of this paragraph:

4.1. if the originator or the addressee has more than one place of business, the place of business is that which has the closest relationship to the underlying transaction or, where there is no underlying transaction, the principal place of business;

4.2. if the originator or the addressee does not have a place of business, reference is to be made to its habitual residence.

### **CHAPTER IV** **ESTABLISHMENT AND INFORMATION REQUIREMENTS**

#### **Article 15** **Establishment and Authorization**

1. Information Society services are any service normally provided for remuneration, at a distance, by electronic means and at the individual request of a recipient of services.

2. This Law shall not apply to:

2.1. services not provided "at a distance";

2.2. services provided in the physical presence of the provider and the recipient, even if they involve the use of electronic devices:

2.2.1. medical examinations or treatment at a doctor's surgery using electronic equipment where the patient is physically present;

2.2.2. consultation of an electronic catalogue in a shop with the customer on site; ticket reservation;

2.2.3. electronic games made available in a video-arcade where the customer is physically present.

2.3. services not provided "by electronic means";

2.4. services having material content even though provided via electronic devices:

2.4.1. automatic cash or ticket dispensing machines (banknotes, rail tickets);

2.4.2. access to road networks, car parks, etc., charging for use, even if there are electronic devices at the entrance/exit controlling access and/or ensuring correct payment is made.

2.5. off-line services: distribution of CDROMs or software on diskettes;

2.6. services which are not provided via electronic processing or inventory systems, including, but not limited to:

2.6.1. voice telephony services;

2.6.2. telefax/telex services;

2.6.3. services provided via voice telephony or fax;

2.6.4. telephone/telefax consultation of a doctor;

2.6.5. telephone/telefax consultation of a lawyer;

2.6.6. telephone/telefax direct marketing.

2.7. services not supplied "at the individual request of a recipient of services";

2.8. services provided by transmitting data without individual demand for simultaneous reception by an unlimited number of individual receivers (point to multipoint transmission):

2.8.1. radio broadcasting services;

2.8.2. television broadcasting services;

2.8.3. teletext provided by television broadcasters;

2.8.4. all other broadcasting services as defined by the respective law on electronic communications.

3. The provision of Information Society Services shall not require prior authorization or any other requirement having equivalent effect, with the exception of:

3.1. service providers utilizing their own infrastructure shall obtain authorizations pursuant to the applicable law on electronic communications;

3.2. service providers offering financial or insurance services pursuant to the applicable laws for such services.

### **Article 16 General Information to be provided by the Service Provider**

1. The service provider shall offer easily, directly and permanently accessible to the recipients of the service and competent authorities, for the following information:

1.1. the name of the service provider;

1.2. the geographic address at which the service provider is established;

1.3. the details of the service provider, including the electronic mail address and universal record locator (URL) of the service provider, which allow him to be contacted rapidly and communicated with in a direct and effective manner;

1.4. the trade register in which the service provider is entered and his registration number;

1.5. the particulars of the relevant supervisory authority (where the activity is subject to an authorization scheme);

1.6. for regulated professions:

1.6.1. any professional body or similar institution with which the service provider is registered;

1.6.2. the professional title and the authority by(from) it has been granted;

1.6.3. a reference to the applicable professional rules in the jurisdiction of establishment and the means to access them;

1.7. VAT – tax identification number (if applicable).

2. Where information society services refer to prices, these are to be indicated unambiguously and must indicate whether they are inclusive of tax and delivery costs

## **CHAPTER V COMMERCIAL COMMUNICATIONS**

### **Article 17 Information to be provided**

1. Commercial communications which are part of an Information Society service should comply at least with the following conditions:

- 1.1. the commercial communications need to be clearly identifiable as such;
- 1.2. the natural or legal person on whose behalf the commercial communication is made need to be clearly identifiable;
- 1.3. promotional offers (discounts, premiums and gifts) need to be clearly identifiable as such, and the conditions which are to be met to qualify for them, shall be easily accessible and be presented clearly and unambiguously;
- 1.4. promotional competitions or games, where permitted in the jurisdiction where the service provider is established, need to be clearly identifiable as such, and the conditions for participation, shall be easily accessible and be presented clearly and unambiguously;

**Article 18**  
**Unsolicited Commercial Communication**

1. Unsolicited commercial communications by electronic mail are not permitted unless e-mail recipient does not give prior consent.
2. Service providers shall consult regularly and respect the opt in registers in which recipients don't wish to receive such commercial communications, can register themselves.

**Article 19**  
**Regulated Professions**

1. The use of commercial communications which are part of an Information Society service provided by professionals are permitted subject to compliance with the professional rules regarding the dignity and honor of the profession, professional secrecy, fairness towards clients and other members of the profession.
2. Professional bodies and associations are encouraged to establish codes of conduct which are fully compliant with European and international standards.

**CHAPTER VI**  
**CONTRACTS CONCLUDED BY ELECTRONIC MEANS**

**Article 20**  
**Information to be provided**

1. The following information is to be given clearly comprehensively and unambiguously by the service provider prior to the order being placed by the recipient of the service, except when otherwise agreed by parties who are not consumers:
  - 1.1. the different technical steps to follow to conclude the contract;
  - 1.2. whether or not the concluded contract will be filed by the service provider and whether it will be accessible;
  - 1.3. the technical means for identifying and correcting input errors prior to the placing of the order;
  - 1.4. the languages offered for the conclusion of the contract.

2. Except when otherwise agreed by parties who are not consumers, the service provider indicates any codes of conduct to which he subscribes and shows how these codes can be consulted electronically.

3. The provisions in paragraphs 1. and 2. of this Article do not apply to contracts concluded exclusively by exchange of electronic mail or individual communications.

4. Contract terms and general conditions provided to the recipient must be made available in a way that allows him to store and reproduce them.

### **Article 21 Placing of the Order**

1. Except when otherwise agreed by parties who are not consumers, the service provider who receives an order through technological means has to acknowledge the receipt of the recipient's order without undue delay and by electronic means. The order and the acknowledgement are deemed to be received when the parties to whom they are addressed are able to access them.

2. Except when otherwise agreed by parties who are not consumers, the service provider makes available to the recipient of the service appropriate technical, effective and useful means allowing him to identify and correct input errors, prior to the placing of the order.

3. The provisions in paragraphs 1. and 2. of this Article do not apply to contracts concluded exclusively by exchange of electronic mail or by equivalent individual communications.

## **CHAPTER VII CARRIAGE OF GOODS**

### **Article 22 Actions Related to Contracts of Carriage of Goods**

1. This Chapter applies to any action in connection with, or in pursuance of, a contract of carriage of goods, including but not limited to:

1.1. furnishing the marks, number, quantity or weight of goods;

1.2. stating or declaring the nature or value of goods;

1.3. issuing a receipt for goods;

1.4. confirming that goods have been loaded;

1.5. notifying a person of terms and conditions of the contract;

1.6. giving instructions to a carrier;

1.7. claiming delivery of goods;

1.8. authorizing release of goods;

1.9. giving notice of loss of, or damage to, goods;

1.10. giving any other notice or statement in connection with the performance of the contract;

1.11. undertaking to deliver goods to a named person or a person authorized to claim delivery;

1.12. granting, acquiring, renouncing, surrendering, transferring or negotiating rights in goods;

1.13. acquiring or transferring rights and obligations under the contract.

**Article 23**  
**Transport Documents**

1. Subject to paragraph 3. of this Article, where this Law requires that any action referred to in Article 22 of this Law be carried out in writing or by using a paper document, that requirement is met if the action is carried out by using one or more data messages.

2. Paragraph 1. of this Article applies whether the requirement therein is in the form of an obligation or whether the law simply provides consequences for failing either to carry out the action in writing or to use a paper document.

3. If a right is to be granted to, or an obligation is to be acquired by, one person and no other person, and if the law requires that, in order to effect this, the right or obligation must be conveyed to that person by the transfer, or use of, a paper document, that requirement is met if the right or obligation is conveyed by using one or more data messages, provided that a reliable method is used to render such data message or messages unique.

4. For the purposes of paragraph 3. of this Article, the standard of reliability required shall be assessed in the light of the purpose for which the right or obligation was conveyed and in the light of all the circumstances, including any relevant agreement.

5. Where one or more data messages are used to effect any action in subparagraphs 1.6. and 1.7. paragraph 1. of Article 22 of this law, no paper document used to effect any such action is valid unless the use of data messages has been terminated and replaced by the use of paper documents. A paper document issued in these circumstances shall contain a statement of such termination. The replacement of data messages by paper documents shall not affect the rights or obligations of the parties involved.

6. If a rule of this Law is compulsorily applicable to a contract of carriage of goods which is in, or is evidenced by, a paper document, that rule shall be applicable to such a contract of carriage of goods which is evidenced by one or more data messages by reason of the fact that the contract is evidenced by such data message or messages instead of by a paper document.

**CHAPTER VIII**  
**LIABILITY OF INTERMEDIARY SERVICE PROVIDERS**

**Article 24**  
**Mere Conduit**

1. When an Information Society service provider offers a service that consists of the transmission in a communication network of information from the recipient of the service or the provision of access to a communication network, the service provider is not liable for the information transmitted, on condition that he:

1.1. does not initiate the transmission;

1.2. does not select the receiver of the transmission;

1.3. does not select or modify the information contained in the transmission.

2. The acts of transmission and of access referred to in paragraph 1. of this Article include the automatic, intermediate and transient storage of the information transmitted in so far as this takes place for the sole purpose of carrying out the transmission in the communication network, and provided that the information is not stored for any period longer than is reasonably necessary for the transmission.

#### **Article 25 Caching**

1. When an Information Society service provider offers a service that consists of the transmission in a communication network of information for the recipient of the service, then the service provider is not liable for the automatic, intermediate and temporary storage of that information, storage performed for the sole purpose of making more efficient the information's onward transmission to other recipients of the service upon their request, in case that:

1.1. provider does not modify the information;

1.2. provider applies the conditions on access to the information;

1.3. provider applies rules regarding the updating of the information, specified in a recognized manners and widely used in industry;

1.4. provider does not interfere with the lawful use of technology, widely recognized and used by industry, to obtain data on the use of the information;

1.5. provider acts immediately to remove or prohibit access to the information it has stored upon obtaining actual knowledge of the fact that the information at the initial source of the transmission has been removed from the network, or access to it has been prohibited, or that a court or an administrative authority has ordered such removal or prohibition.

#### **Article 26 Hosting**

1. When an Information Society service provider offers the storage of information provided by the recipient of the service, he is not liable for the information stored at the request of a recipient of the service, in case that:

1.1. service provider does not have knowledge of illegal activity or information and, as regards of claims for damages, is not aware of facts or circumstances from which the illegal activity or information is apparent; or

1.2. service provider upon obtaining the abovementioned knowledge, shall act expeditiously to remove or to prohibit access to such information.

#### **Article 27 Liability for damages resulting from removing or disabling access to information**

1. Any person who notifies the Information Society service provider of illegal activity or information is liable for damages resulting from the removing or disabling access to the information, referred to in, subparagraph 1.2 paragraph 1. Article 26 of this law when:

1.1. he did not act in good faith; or

1.2. he benefited from the actions of the Information Society service provider; or

1.3. he knew, or should have known, that the information or activity was not illegal.

**Article 28**  
**Exemption from General Obligation for Monitoring**

1. Information Society service providers, when providing the services covered by the Articles in this Chapter, have no general obligation to monitor the information which they transmit or store, nor a general obligation actively to seek facts or circumstances indicating illegal activity.

2. Information society service providers shall promptly inform the public authorities competent according to the legislation in force in the matter alleged illegal activity undertaken or information provided by recipient of their service and shall grant to any such authority upon request information enabling the identification of recipients in their services with whom they have storage agreements.

3. Provided that nothing in this Article shall be interpreted as imposing an obligation on Information Society service providers to monitor the information which they transmit or store or to actively seek fact or circumstances indicating illegal activity in connection with activities described in Articles 24, 25 and 26 of this Law.

**CHAPTER IX**  
**DISTANCE CONTRACTS**

**Article 29**  
**Definition and Scope**

1. Distance Contract is a contract concerning goods or services concluded between a supplier and a consumer under an organized distance sales or service-provision scheme run by the supplier who makes use of means of distance communication up to and including the moment at which the contract is concluded.

2. Distance communication includes any means that are used for the conclusion of a contract without the simultaneous presence of the supplier and the consumer. Examples include, but are not limited to:

- 2.1. addressed and unaddressed printed matter;
- 2.2. standard letter;
- 2.3. press advertising with order form;
- 2.4. catalogue;
- 2.5. telephone with human intervention;
- 2.6. telephone without human intervention (automatic calling machine or audio text);
- 2.7. radio;
- 2.8. videophone (telephone with screen);

- 2.9. videotext (microcomputer and television screen) with keyboard or touch screen;
- 2.10. electronic mail;
- 2.11. facsimile machine (fax);
- 2.12. television (teleshopping).

### **Article 30 Exemptions**

1. This Law does not apply to contracts:

- 1.1. relating to any financial or insurance services will which the distance marketing of consumer financial services applies;
- 1.2. concluded by means of automatic vending machines or automated commercial premises;
- 1.3. concluded with telecommunications service providers through the use of public payphones;
- 1.4. concluded for the construction and sale of immovable property or relating to other immovable property rights, except for rental;
- 1.5. concluded at an auction.

2. The requirements related to Article 31., 32. , 33. and 34. of this Law do not apply to:

- 2.1. contracts for the supply of foodstuffs, beverages or other goods intended for everyday consumption supplied to the home of the consumer, to his residence or to his workplace by regular rounds men;
- 2.2. contracts for the provision of accommodation, transport, goods supply or leisure services, where the supplier undertakes according to contract exceptionally, in specific circumstances in the case of extraordinary situations, the supplier will be released of obligation to refund he consumer the sums he has paid.

### **Article 31 Prior Information**

1. At a reasonable time prior to the conclusion of any distance contract, the consumer must be provided with the following information:

- 1.1. the identity of the supplier and, in the case of contracts requiring payment in advance, his address;
- 1.2. the main characteristics of the goods and services;
- 1.3. the price of the goods or services including all taxes;
- 1.4. delivery costs, where appropriate;
- 1.5. the arrangements for payment, delivery or performance;

- 1.6. the existence of a right of withdrawal;
  - 1.7. the cost of using the means of distance communication, where it is calculated other than at the basic rate;
  - 1.8. the period for which the offer or the price remains valid;
  - 1.9. where appropriate, the minimum duration of the contract in the case of contracts for the supply of products or services to be performed permanently or recurrently.
2. The above mentioned information, commercial aim of which should be clear, shall be provided in a clear and comprehensible manner conformable communication means used in distance. A due regard must be given to the principles of confidence in commercial transactions, and the principles for protection of those who are unable, to give their consent, pursuant to the applicable law (e.x. minors).
3. In the case of telephone communications, the identity of the supplier and the commercial purpose of the call must be made explicitly clear at the beginning of all conversations with the consumer.

### **Article 32 Written Confirmation of Information**

1. The consumer must receive written confirmation or confirmation in another durable medium available and accessible to him of the information mentioned in Article 31 of this Law. If this information is not provided prior to the conclusion of the contract, then it should be provided as soon as possible during the period of fulfillment of the contract and at the latest at the time of delivery of goods.
2. In any event, the following must be provided:
  - 2.1. written information on the conditions and procedures for exercising the right of withdrawal;
  - 2.2. the geographical address of the place of business of the supplier to which the consumer may address any complaints;
  - 2.3. information on after-sales services and guarantees which exist;
  - 2.4. the conclusion for canceling the contract, where it is of unspecified duration or a duration exceeding one (1) year.
3. This information is not needed for services which are performed through the use of a means of distance communication, where they are supplied on only one occasion and are invoiced by the service provider of the means of distance communication. The consumer shall in all cases be able to obtain the geographical address of the place of business of the supplier to which he may address any complaints.

### **Article 33 Right of Withdrawal**

1. For any distance contract the consumer shall have a period of at least seven (7) working days in which to withdraw from the contract.
2. The only charge for the consumer because of the exercise of his right of withdrawal is the direct cost of returning the goods.

3. The period for exercise of this right shall begin:

3.1. in the case of goods, from the day of receipt by the consumer where the obligations regarding written confirmation of information have been fulfilled;

3.2. in the case of services, from the day of conclusion of the contract or from the day on which the obligations regarding written confirmation of information were fulfilled if they are fulfilled after conclusion of the contract, provided that this period does not exceed the three (3) months.

4. If the supplier has failed to fulfill the obligations regarding written confirmation of information, the period shall be three (3) months. The period shall begin:

4.1. in the case of goods, from the day of receipt by the consumer;

4.2. in the case of services, from the day of conclusion of the contract.

5. If the mandatory written confirmation of information is supplied within this three (3) month period, the seven (7) working day period, according to paragraph 1. of this Article will begin from that moment.

6. Where the right of withdrawal has been exercised by the consumer, the supplier shall be obliged to reimburse the sums paid by the consumer free of charge. The only charge for the consumer is the direct cost of returning the goods. Such reimbursement must be carried out not later than thirty (30) days.

7. Unless the parties have agreed otherwise, the consumer may not exercise the right of withdrawal in respect of contracts:

7.1. for the provision of services if performance has begun, with the consumer's agreement, before the end of the seven (7) working day period according to paragraph 1. of this Article;

7.2. for the supply of goods made to the consumer's specifications or clearly personalized or which, by reason of their nature, can't be returned or are liable to deteriorate or expire rapidly;

7.3. for the supply of audio or video recordings or computer software which were unsealed by the consumer;

7.4. for the supply of newspapers, periodicals and magazines;

7.5. for games and lottery services.

8. If the price of goods or services is fully or partly covered by credit granted by the supplier, or if that price is fully or partly covered by credit granted to the consumer by a third party on the basis of an agreement between the third party and the supplier, the credit agreement shall be cancelled without any penalty if the consumer exercises his right to withdraw from the contract.

#### **Article 34 Performance**

1. Unless the parties have agreed otherwise, the supplier must execute the order within a maximum of thirty (30) days from the day following that on which the consumer forwarded his order to the supplier.

2. Where a supplier does not fulfill his side of the contract on the grounds that the goods or services ordered are unavailable, the consumer must be informed of this situation and must be able to obtain a refund of any sums he has paid as soon as possible and not later than thirty (30) days.

3. The supplier may provide the consumer with goods or services of equivalent quality and price provided that this possibility was provided for prior to the conclusion of the contract or in the contract. The cost of returning the goods following exercise of the right of withdrawal shall, in this case, be borne by the supplier, and the consumer must be informed about this. In such cases the supply of goods or services may not be deemed to constitute inertia selling pursuant to Article 36 of this law.

### **Article 35 Cancellation of Payment by Card in Fraudulent Events**

1. Consumer shall be entitled:

1.1. to request cancellation of a payment where fraudulent use has been made of his payment card in connection with distance contracts covered by this Law;

1.2. in the event of fraudulent use, to be recredited with the sums paid or have them returned.

### **Article 36 Inertia Selling**

1. It is prohibited to supply goods or services to a consumer without their being ordered by the consumer beforehand, where such supply involves a demand for payment.

2. A consumer shall not be required to provide anything in cases of unbidden supply. The absence of a reply does not constitute an admission in these cases.

### **Article 37 Prior Consent of the Consumer on the use of Certain Means of Distance Communication**

1. The consumer should give a prior consent allowing the supplier to use:

1.1. automated calling system without human intervention (automatic calling machine);

1.2. facsimile machine (fax).

2. Other means of distance communication, which allow individual communications, may be used only where there is no clear objection from the consumer.

### **Article 38 Judicial or Administrative Redress**

1. The following bodies may take action under applicable law before the courts or before the competent administrative bodies to ensure that this Law is applied correctly:

1.1. public bodies or their representatives;

1.2. consumer organizations;

1.3. professional organizations.

**Article 39**  
**Binding Nature**

The consumer may not waive the rights conferred on him by this part of this Law. The consumer does not lose the protection granted by this Law by virtue of the choice of the law of an external jurisdiction as the law applicable to the contract.

**CHAPTER X**  
**ELECTRONIC INVOICING**

**Article 40**  
**Required Details on Invoices**

1. The following details are required on invoices in electronic commerce:
  - 1.1. the date of issue;
  - 1.2. a sequential number, based on one or more series, which uniquely identifies the invoice;
  - 1.3. the VAT identification number under which the taxable person supplied the goods or services (if applicable);
  - 1.4. the full name and address of the taxable person and of his customer;
  - 1.5. the quantity, price, and nature of the goods supplied or the extent and nature of the services rendered;
  - 1.6. the date on which the supply of goods or of services was made or completed or the date on which the payment on account was made, insofar as that a date can be determined and differs from the date of issue of the invoice;
  - 1.7. the taxable amount per rate or exemption, the unit price exclusive of tax and any discounts or rebates if they are not included in the unit price;
  - 1.8. the VAT rate applied;
  - 1.9. the VAT amount payable.
2. It is not required that invoices be signed.
3. The amounts which appear on the invoice may be expressed in any currency, provided that the amount of tax to be paid is expressed in the Euro.

**Article 41**  
**Invoices on Paper or by Electronic Means**

1. Invoices may be sent either on paper or, subject to an acceptance by the customer, by electronic means. Invoices sent by electronic means shall be acceptable in Kosovo provided that the authenticity of the origin and integrity of the contents are guaranteed:

1.1. by means of an advanced electronic signature; or

1.2. by means of an advanced electronic signature to be based on a qualified certificate and created by a secure-signature-creation device; or

1.3. by means of electronic data interchange (EDI) when the agreement relating to the exchange provides for the use of procedures guaranteeing the authenticity of the origin and integrity of the data.

1.4. by other electronic means adopted by the Minister through a sub-legal act.

2. Invoices may be sent by other electronic means subject to the explicit acceptance by the customer concerned.

3. When batches containing several invoices are sent to the same recipient by electronic means, the details that are common to the individual invoices may be mentioned only once if, for each invoice, all the information is accessible.

#### **Article 42 Storage of Invoices**

1. Every taxable person shall ensure that copies of invoices issued by himself and all the invoices which he has received are stored, pursuant to the Tax Law of Kosovo as established by the Ministry of Finance.

2. The taxable person may decide the place of storage provided that he makes the invoices or information stored there available to the competent authorities whenever they request.

3. The authenticity of the origin and integrity of the content of the invoices, as well as their readability, must be guaranteed throughout the storage period. In order to ensure that these conditions are met, invoices may be stored in the original form in which they were sent, whether paper or electronic. When invoices are stored by electronic means, the data guaranteeing the authenticity of the origin and integrity of the content shall also be stored.

4. The Ministry of Finance shall determine the period for which taxable persons must store invoices relating to goods or services supplied in their territory and invoices received by taxable persons established in Kosovo.

5. Transmission and storage of invoices by electronic means transmission or making available to the recipient, and storage using electronic equipment for processing (including digital compression) and storage of data, and employing wires, radio transmission, optical technologies or other electromagnetic means.

### **CHAPTER XI ELECTRONIC PAYMENTS**

#### **Article 43 Implementation of Electronic payments**

1. This Law applies to electronic payments and sets out the conditions which should be fulfilled if the new, electronic means of payment are to be developed for the benefit of all economic partners and are to afford:

- 1.1. for consumers, security and convenience;
  - 1.2. for traders and issuers, greater security and productivity;
  - 1.3. for the development of industry in Kosovo.
2. The principles of fair practice must be observed by all those who bring card payment systems into operation or make use of them.
3. The technological development of electronic means of payment should have an eye to their European dimension: such means must be as widely interoperable as possible, to avoid having isolated systems and, hence, a partitioned market.
4. This Law shall not apply to:
- 4.1. cards not having an equivalent of monetary value;
  - 4.2. cards issued by a specific company, if that company is the only one where that card or the value on it can be used.

#### **Article 44 Contracts**

1. Contracts concluded by issuers or their agents, with traders and cardholder shall be in writing and must be the result of a prior application. They shall set out in detail the general and specific conditions of the agreement.
2. Contracts shall be drawn up in the official languages of Republic of Kosova.
3. Any scale of charges must be determined in a transparent manner, taking account of actual costs and risks and without involving any restriction of competition.
4. All conditions, provided they are in conformity with the applicable law, shall be freely negotiable and clearly stipulated in the contract.
5. Conditions specific to termination of a contract must be stated and brought to the notice of the parties prior to such contract being concluded.

#### **Article 45 Interoperability**

Interoperability shall be full and complete, so that traders and consumers can join the network(s) or contract with the issuer(s) of their choice, with each terminal being able to process all cards.

#### **Article 46 Equipment**

1. Electronic payment terminals shall register, control and transmit payments and may be integrated into a point-of-sale terminal.
2. Traders have the possibility, if they wish, to install a single or multi-card-terminal.
3. Traders shall be free to choose which point-of-sale terminal they will install. They shall be at liberty either to rent or purchase such equipment, provided only that it is certified as satisfying the requirements of the whole payment system and can be used on an interoperable basis.

**Article 47**  
**Data Protection and Security**

1. Electronic payments are irreversible. An order given by means of a payment card shall be irrevocable and may not be countermanded.
2. The information transmitted, at the time of payment, to the trader's bank and subsequently to the issuer shall not under any circumstances prejudice the protection of privacy. It shall be strictly limited to that normally laid down for cheques and transfers.
3. Any problems whatsoever that arise in connection with the protection of information or with security shall be openly acknowledged and cleared up at whatever stage in the contract between the parties.
4. Contracts must not restrict trader's freedom of operation or freedom to compete.

**Article 48**  
**Fair Access to the System**

1. Irrespective of their economic size, all establishments concerned shall be allowed fair access to the system of electronic payment. A trader may be refused access only for reasons consistent with the legislation in force.
2. There shall be no unwarranted difference in the remuneration for services concerning transactions within Kosovo as well as with the remuneration for the same services concerning transnational transactions with other countries, especially in border regions.

**Article 49**  
**Relations between Issuers and Traders**

1. To promote mutual access among different card systems, contracts between card issuers and traders shall contain no exclusive trading clause requiring the trader to operate only the system with which he has contracted an agreement.
2. Contracts with traders shall admit effective competition between the various issuers. Compulsory provisions shall be limited strictly to technical requirements for ensuring that the system functions properly.

**Article 50**  
**Relations between Issuers and Consumers**

Cardholders shall take all reasonable precautions to ensure the safety of the card issued and shall observe the special conditions (loss or theft) in the contract which they have signed.

**Article 51**  
**Relations between Traders and Consumers**

Traders shall display, in a fully visible manner, the signs of the companies to which they are affiliated, related to that they shall be obliged to accept such cards.

**CHAPTER XII**  
**ELECTRONIC SIGNATURES**

**Article 52**

## **Equal Treatment of Signature Technologies**

Nothing in this Law, except Article 54 of this law, shall be applied so as to exclude, restrict or deprive of legal effect any method of creating an electronic signature that satisfies the requirements referred to in paragraph 1. Article 55 of this law, or otherwise meets the requirements of applicable law.

### **Article 53 Variation by Agreement**

The provisions of this Chapter of the Law may be derogated from or their effect may be varied by agreement, unless that agreement would not be valid or effective under applicable law.

## **CHAPTER XIII USE OF SIGNATURES**

### **Article 54 Compliance with a Requirement for Signature**

1. An electronic signature is considered to be reliable for the purpose of satisfying the requirement referred to in Article 6 of this Law if:

- 1.1. the requirements for an advanced electronic signature are met;
- 1.2. it is based on a qualified certificate;
- 1.3. it is created by a secure signature creation device.

2. An electronic signature is not considered to be insufficiently reliable on the sole ground that:

- 2.1. it is not based on a qualified certificate, or
- 2.2. it not based upon a qualified certificate issued by an accredited certification service provider, or
- 2.3. is not created by a secure signature creation device.

3. Provided that if the electronic signature is in the form of an advanced electronic signature, which is based on a qualified certificate and is created by a secure creation device, it shall for all intents and purposes of this Law be presumed to be the signature of the signatory.

4. Paragraph 1. of this Article does not limit the ability of any person:

- 4.1. to establish in any other way, for the purpose of satisfying the requirement referred to in Article 6 of this law, the reliability of an electronic signature; or
- 4.2. to adduce evidence of the non-reliability of an electronic signature.

### **Article 55 Practicability**

1. The Minister may determine by sub-legal act which electronic signatures satisfy the provisions of paragraph 2. Article 55 of this Law and may make regulations in order to give fuller effect to the acceptance and use of electronic signatures

2. Any determination made under paragraph 1. of this Article shall be consistent with recognized international standards and applicable European legislation.

3. Nothing in this Article affects the operation of the rules of private international law.

#### **Article 56 Conduct of Signatory**

1. Where signature creation data can be used to create a signature that has legal effect, each signatory shall:

1.1. exercise reasonable care to avoid unauthorized use of its signature creation data;

1.2. without undue delay, utilize means made available by the certification service provider pursuant to Article 57 of this Law, or otherwise use reasonable efforts, to notify any person that may reasonably be expected by the signatory to rely on or to provide services in support of the electronic signature if:

1.2.1. the signatory knows that the signature creation data have been compromised; or

1.2.2. the circumstances known to the signatory give rise to a substantial risk that the signature creation data may have been compromised;

1.3. where a certificate is used to support the electronic signature, exercise reasonable care to ensure the accuracy and completeness of all material representations made by the signatory that are relevant to the certificate throughout its life cycle or that are to be included in the certificate.

2. A signatory shall bear the legal consequences of its failure to satisfy the requirements of paragraph 1. of this Article.

#### **Article 57 Conduct of the Certification Service Provider**

1. Where a certification service provider provides services to support an electronic signature that may be used for legal effect as a signature, that certification service provider shall:

1.1. act in accordance with representations made by it with respect to its policies and practices;

1.2. exercise reasonable care to ensure the accuracy and completeness of all material representations made by it that are relevant to the certificate throughout its life cycle or that are included in the certificate;

1.3. provide reasonably accessible means that enable a relying party to ascertain from the certificate:

1.3.1. the identity of the certification service provider;

1.3.2. that the signatory that is identified in the certificate had control of the signature creation data at the time when the certificate was issued;

1.3.3. that signature creation data were valid at or before the time when the certificate was issued;

1.4. provide reasonably accessible means that enable a relying party to ascertain, where relevant, from the certificate or otherwise:

1.4.1. the method used to identify the signatory;

1.4.2. any limitation on the purpose or value for which the signature creation data or the certificate may be used;

1.4.3. that the signature creation data are valid and have not been compromised;

1.4.4. any limitation on the scope or extent of liability stipulated by the certification service provider;

1.4.5. whether means exist for the signatory to give notice pursuant to subparagraph 1. 2 paragraph 1. Article 56 of this Law;

1.4.6. whether a timely revocation service is offered;

1.5. where services under subparagraph 1.4.5 of this Article are offered, provide a means for a signatory to give notice pursuant to paragraph 1.2 paragraph 1. Article 56 of this Law and, where services under subparagraph 1.4.6 of this Article are offered, ensure the availability of a timely revocation service;

1.6 utilize trustworthy systems, procedures and human resources in performing its services.

2. A certification service provider shall bear the legal consequences of its failure to satisfy the requirements of paragraph 1. of this Article.

3. Certification-service-providers, issuing qualified certificates, shall:

3.1. demonstrate the reliability necessary for providing certification services;

3.2. ensure the operation of a prompt and secure directory and a secure and immediate revocation service;

3.3.ensure that the date and time when a certificate is issued or revoked can be determined precisely;

3.4. verify, by appropriate means in accordance with applicable law, the identity and, if applicable, any specific attributes of the person to which a qualified certificate is issued;

3.5. employ personnel who possess the expert knowledge, experience, and qualifications necessary for the services provided, in particular competence at managerial level, expertise in electronic signature technology and familiarity with proper security procedures; they must also apply administrative and management procedures which are adequate and correspond to recognized standards;

3.6. use trustworthy systems and products which are protected against modification and ensure the technical and cryptographic security of the process supported by them;

3.7. take measures against forgery of certificates, and, in cases where the certification-service-provider generates signature-creation data, guarantee confidentiality during the process of generating such data;

3.8. maintain sufficient financial resources to operate in conformity with the requirements laid down in respective European legislation for Electronic Signature, in particular to bear the risk of liability for damages, for example, by obtaining appropriate insurance;

3.9. record all relevant information concerning a qualified certificate for an appropriate period of time, in particular for the purpose of providing evidence of certification for the purposes of legal proceedings. Such recording may be done electronically;

3.10. not store or copy signature-creation data of the person to whom the certification-service-provider provided key management services;

3.11. before entering into a contractual relationship with a person seeking a certificate to support his electronic signature inform that person by a durable means of communication of the precise terms and conditions regarding the use of the certificate, including any limitations on its use, the existence of a voluntary accreditation scheme and procedures for complaints and dispute settlement. Such information, which may be transmitted electronically, must be in writing and in readily understandable language. Relevant parts of this information must also be made available on request to third-parties relying on the certificate;

3.12. use trustworthy systems to store certificates in a verifiable form so that only authorized persons can make entries and changes, information can be checked for authenticity, certificates are publicly available for retrieval in only those cases for which the certificate-holder's consent has been obtained, and any technical changes compromising these security requirements are apparent to the operator.

#### **Article 58 Trusted list**

1. The Ministry shall maintain a register of certification service providers established in Kosovo.
2. The register referred to in paragraph 1. of this Article, shall be available to anyone and machine readable by standards used in the European Union, and it shall be reliable, current and secure.
3. Certification service providers may request a registration on this list if they meet the requirements set out in Article 57 of this law and is established in Kosovo and provide to that end, all information the Ministry deems relevant.
4. Certification service providers shall expeditiously notify the Minister of changes in the relevant information, including the termination of the service or their inability to comply with any of the requirements set out in Article 57 of this Law.

#### **Article 59 Supervisory Authority**

1. The Ministry may authorize a public or private body, to maintain the register and exercise supervisory authority.
2. The Ministry may, in the context of the supervision of certification service providers established in Kosovo, prescribe on any of the following matters:

- 2.1. the powers and functions of the supervisory authority;
- 2.2. any other matter relating to the supervisory authority which may appear to the Ministry to be necessary or desirable.

#### **Article 60 Trustworthiness**

1. For the purposes of sub-paragraph 1.6. paragraph 1. Article 57 of this Law in determining whether, or to what extent, any systems, procedures and human resources utilized by a certification service provider are trustworthy, regard may be had to the following factors:

- 1.1. financial and human resources, including existence of assets;
- 1.2. quality of hardware and software systems;
- 1.3. procedures for processing of certificates and applications for certificates and retention of records;
- 1.4. availability of information to signatories identified in certificates and to potential relying parties;
- 1.5. regularity and extent of audit by an independent body;
- 1.6. the existence of a declaration by the Ministry, the supervisory authority, an accreditation body or the certification service provider regarding compliance with or existence of the foregoing; or
- 1.7. any other relevant factor.

#### **Article 61 Conduct of the Relying Party**

1. Notwithstanding paragraph 3. of Article 12 of this Law, a relying party shall bear the legal consequences of its failure:

- 1.1. to take reasonable steps to verify the reliability of an electronic signature; or
- 1.2. where an electronic signature is supported by a certificate, to take reasonable steps:
  - 1.2.1. to verify the validity, suspension or revocation of the certificate; and
  - 1.2.2. to observe any limitation with respect to the certificate.

#### **Article 62 Recognition of Foreign Certificates and Electronic Signatures**

1. In determining whether, or to what extent, a certificate or an electronic signature is legally effective, no regard shall be had:

- 1.1. to the geographic location where the certificate is issued or the electronic signature created or used; or

- 1.2. to the geographic location of the place of business of the issuer or signatory.
2. A certificate issued outside of Kosovo shall have the same legal effect in Kosovo as a certificate issued in Kosovo if it offers a substantially equivalent level of reliability.
3. An electronic signature created or used outside of Kosovo shall have the same legal effect in Kosovo as an electronic signature created or used in Kosovo if it offers a substantially equivalent level of reliability.
4. In determining whether a certificate or an electronic signature offers a substantially equivalent level of reliability for the purposes of paragraph 2. or 3. of this Article, regard shall be had to recognized international standards and to any other relevant factors.
5. Certificates issued by foreign certification service providers are equal to certificates issued by certification service providers in Kosovo, if the foreign certification service provider is:
  - 5.1. accredited in a member state of the European Union, or
  - 5.2. if their certificates are guaranteed by a certification service provider established in the European Union.
6. Where, notwithstanding paragraphs 2., 3. and 4 of this Article, parties agree, as between themselves, to the use of certain types of electronic signatures or certificates, that agreement shall be recognized as sufficient for the purposes of cross-border recognition, unless that agreement would not be valid or effective under applicable law.

## **CHAPTER XIV PROTECTION OF SYSTEMS OF INFORMATION SOCIETY SERVICES**

### **Article 63 Systems of information society services**

Protection of systems of information society services aims to improve cooperation between judicial and other competent authorities, including the police and other specialized law enforcement services of Kosovo, through approximating rules on Criminal Code in Republic of Kosovo in the area of attacks against Information Systems and data transfer.

### **Article 64 Illegal Access to Information Systems**

1. The intentional access, without right, to the whole or any part of an information system is punishable as a criminal offense where it is committed:
  - 1.1. against any part of an information system which is subject to specific protection measures; or
  - 1.2. with the intent to cause damage to a natural or legal person; or
  - 1.3. with the intent to result in an economic benefit.
2. The provisions of paragraph 1. of this Article specifically apply also to data interception.
3. The following intentional conduct, without right, is punishable as a criminal offense:

3.1 the serious hindering or interruption of the functioning of an information system by inputting, transmitting, damaging, deleting, deteriorating, altering, suppressing or rendering inaccessible computer data;

3.2 the deletion, deterioration, alteration, suppression or rendering inaccessible of computer data on an information system where it is committed with the intention to cause damage to a natural or legal person.

4. When the criminal offense has been committed regarding paragraph 1., 2. and 3. of this Article, the offender is convicted with one (1) to five (5) years by imprisonment.

5. Legal Person is responsible for committing the criminal offense as foreseen in paragraph 1., 2. and 3. of this Article and is punishable according to the law.

#### **Article 65** **Instigation, Aiding, Abetting and Attempt**

The intentional instigation of, aiding or abetting an offense referred to in Article 64 of this law is punishable.

#### **Article 66** **Aggravating Circumstances**

1. The criminal offenses referred to in paragraph 1.2 and 3 Article 64 of this law are punishable by imprisonment of no less than five (5) years when they are committed under the following circumstances:

1.1. the criminal offense has been committed within the framework of a criminal organization as defined in “European Union Joint Action 98/733/ JHA” of 21 December 1998 on making it a criminal offense to participate in a criminal organization in the Member States of the European Union, apart from the penalty level referred to therein;

1.2. the criminal offense caused, or resulted in, substantial direct or indirect economic loss, physical harm to a natural person or substantial damage to part of the critical infrastructure of Kosovo;

1.3. the offense resulted in substantial proceeds.

2. The criminal offenses referred to in paragraph 1., 2. and 3. Articles 64 of this law are punishable by custodial sentences higher than those foreseen under paragraph 4. of the Article 64 of this Law, when the offender has been convicted of such an offense by a final judgment in the Court of Justice of the European Union.

#### **Article 67** **Exchange of Information**

For the purpose of exchange of information relating to the offenses referred to in Articles 64 and 66 of this Law, and in accordance with applicable law the contact point will be established as foreseen in the Law on Prevention and Fight of the Cyber Crime.

### **CHAPTER XV** **FINAL PROVISIONS**

#### **Article 68** **General Principles**

The matters, not expressly settled in this Law, will be settled in conformity with the general principles on which this law is based.

**Article 69**  
**Implementation of the Law**

The Ministry and TRA in terms of twelve (12) months shall draw sub-legal acts for the implementation of this Law.

**Article 70**  
**Repeal Provision**

This Law repeals the Law no.2005/02-L23 on Information Society Services.

**Article 71**  
**Entry to the Force**

This Law shall enter into force fifteen (15) days after the publication in the Official Gazette of Republic of Kosova.

**Law No. 04/L-094**  
**15 March 2012**

**Promulgated by Decree No.DL-010-2012, dated 02.04.2012, President of the Republic of Kosovo Atifete Jahjaga.**