UNITED NATIONS
United Nations Interim
Administration Mission
in Kosovo

UNMIK

NATIONS UNIES
Mission d'Administration
Intérimaire des Nations Unies au
Kosovo

PROVISIONAL INSTITUTIONS OF SELF GOVERNMENT

KUVENDI I KOSOVËS
СКУПШТИНА КОСОВА
ASSEMBLY OF KOSOVO

Law No.02/L-23

ON THE INFORMATION SOCIETY SERVICES

Assembly of Kosovo,

Pursuant to Constitutional Framework of the Provisional Self-Government in Kosovo, in particular Chapters 5.1,(l), 9.1.26 (a), 9.3.3, For the purpose of adopting an appropriate legal framework with the outputs of electronic information system, international standards , development , functioning, increase of quality and the security over the scope of information society services,

Hereby adopts the following:

LAW ON THE INFORMATION SOCIETY SERVICES

PART ONE – ELECTRONIC COMMERCE IN GENERAL

Chapter I
General Provisions

Article 1
Purpose and Scope

1.1. This Law shall make electronic documentation legally equivalent to its traditional counterpart in paper format, in order to facilitate commercial activities 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). It is based on the model law developed by the United Nations Commission on International Trade Law (UNCITRAL).

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

a) contracts that create or transfer rights in real estate, except for rental rights;

b) contracts requiring by law the involvement of courts, public authorities or professions exercising public authority;

c) contracts of surety ship granted and on collateral securities furnished by persons acting for purposes outside their trade, business or profession;

d) contracts governed by family law or by the law of succession.

1.3. This Law does not override any rule of law intended for the protection of consumers.

Article 2
Definitions

The following terms, whether in the singular or plural, shall have the meanings stated below:

"**Addressee**" of a data message means 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.

"**Call**" means a connection established by means of a publicly available telephone service allowing two-way communication in real time.

"**Commercial**" means 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:

a) any trade transaction for the supply or exchange of goods or services;
b) distribution agreements;
c) commercial representation or agency;
d) factoring;
e) leasing;
f) construction of works;
g) consulting;
h) engineering;
i) licensing;
j) investment;
k) financing;
l) banking;
m) insurance;
n) exploitation agreement or concession;
o) joint venture and other forms of industrial or business cooperation;
p) carriage of goods or passengers by air, sea, rail or road.

"**Communication**" means 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.

"**Consent**" by a user or subscriber corresponds to the data subject's consent in European Directive 95/46/EC

"**The data subject's consent**" shall mean any freely given specific and informed indication of his wishes by which the data subject signifies his agreement to personal data relating to him being processed.

"**Consumer**" means a credit or debit cardholder, with respect to electronic payments.

"**Controller**" mean 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.

"**Data message**" means 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.

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

"**Electronic mail**" means 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.

"**Electronic payment**" means any payment transaction carried out by means of a card incorporating a magnetic strip, microcircuit or biometric key used at an electronic payment terminal (EPT) or point-of-sale (POS) terminal. This Law does not cover:

a) 'company-specific' cards not covered by the above definition;
b) cards serving purposes other than direct or deferred payment;
c) payments by cheque with bank-card guarantee;
d) payments by card using mechanical processes (invoice slips).

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

"**Intermediary with respect to a particular data message**", means 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.

"**Interoperability**" means a state of affairs whereby cards issued in one Member State and/or belonging to a given card system can be used in other Member States 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.

"Issuer" means any public, banking or credit institution issuing a payment card for electronic use, any production or service.

"**Location data**" means any data processed in an electronic communications network, indicating the geographic position of the terminal equipment of a user of a publicly available electronic communications service.

"**Originator**" of a data message means 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.

"**Personal data**" means any information relating to an identified or identifiable natural person ("data subject"); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity.

"**Processing**" means 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.

"**Processor**" means any natural or legal person, public authority, agency or any other body which processes personal data on behalf of the controller.

"**Trader**" means a distributive trading or service establishment.

"**Traffic data**" means any data processed for the purpose of the conveyance of a communication on an electronic communications network or for the billing thereof.

"**User**" means any natural person using a publicly available electronic communications service, for private or business purposes, without necessarily having subscribed to this service.

"**Value added service**" means any service which requires the processing of traffic data or location data other than traffic data beyond what is necessary for the transmission of a communication or the billing thereof.

Article 3
Variation by Agreement

3.1. As between parties involved in generating, sending, receiving, storing or otherwise processing data messages, and except as otherwise provided, the provisions of Chapter III may be varied by agreement.

3.2. Paragraph (1) 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 legal effect, validity or enforceability solely on the grounds that it is in the form of a data message, nor on the grounds that it is not contained in the data message purporting to give rise to such legal effect, but is merely referred to in that data message.

Article 5
Writing

5.1. Where the law requires information to be in writing, that requirement is met by a data message if the information contained therein is accessible so as to be usable for subsequent reference.

5.2. Paragraph (1) applies whether the requirement therein is in the form of an obligation or whether the law simply provides consequences for the information not being in writing.

Article 6
Signature

6.1. Where the law requires a signature of a person, that requirement is met in relation to a data message if:

(a) a method is used to identify that person and to indicate that person's approval of the information contained in the data message; and

(b) that method is as reliable as was appropriate for the purpose for which the data message was generated or communicated, in the light of all the circumstances, including any relevant agreement.

6.2. Paragraph (1) 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

7.1. Where the law requires information to be presented or retained in its original form, that requirement is met by a data message if:

(a) there exists a reliable assurance as to the integrity of the information from the time when it was first generated in its final form, as a data message or otherwise; and

(b) where it is required that information be presented, that information is capable of being displayed to the person to whom it is to be presented.

7.2. Paragraph (1) 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.

7.3. For the purposes of subparagraph (a) of paragraph (1) the criteria for assessing integrity shall be:

(a) whether the information has remained complete and unaltered, apart from the addition of any endorsement and any change which arises in the normal course of communication, storage and display; and

(b) the standard of reliability required shall be assessed in the light of the purpose for which the information was generated and in the light of all the relevant circumstances.

Article 8
Admissibility and Evidential Weight of Data Messages

8.1. In any legal proceedings, nothing in the application of the rules of evidence shall apply so as to deny the admissibility of a data message in evidence:

(a) on the sole ground that it is a data message; or,

(b) if it is the best evidence that the person adducing it could reasonably be expected to obtain, on the grounds that it is not in its original form.

8.2. Information in the form of a data message shall be given due evidential weight. In assessing the evidential weight of a data message, regard shall be had to the reliability of the manner in which the data message was generated, stored or communicated, to the reliability of the manner in which the integrity of the information was maintained, to the manner in which its originator was identified, and to any other relevant factor.

Article 9
Retention of Data Messages

9.1. Where the law requires that certain messages (documents, records or information) be retained, that requirement is met following condition as:

a) the messages content therein is accessible so as to be usable for subsequent reference; and

b) the data message is retained in the format in which it was generated, sent or received, or in a format which can be demonstrated to represent accurately the information generated, sent or received; and

c) such information, is retained such as enables the identification of the origin and destination of a data message and the date and time when it was sent or received.

9.2. An obligation to retain documents, records or information in accordance with paragraph (1) does not extend to any information the sole purpose of which is to enable the message to be sent or received.

9.3. A person may satisfy the requirement referred to in paragraph (1) by using the services of any other person, provided that the conditions set forth in subparagraphs (a), (b) and (c) of paragraph (1) are met.

Chapter III
Communication of Data Messages

Article 10
Formation and Validity of Contracts

In the context of contract formation, unless otherwise agreed by the parties, an offer and the acceptance of an offer may be expressed by means of data messages. Where a data message is used in the formation of a contract, that contract shall not be denied validity or enforceability on the sole ground that a data message was used for that purpose.

Article 11
Recognition by Parties of Data Messages

As between the originator and the addressee of a data message, a declaration of will or other statement shall not be denied legal effect, validity or enforceability solely on the grounds that it is in the form of a data message.

Article 12
Attribution of Data Messages

12.1. A data message is that of the originator if it was sent by the originator itself.

12.2. As between the originator and the addressee, a data message is deemed to be that of the originator if it was sent:

(a) by a person who had the authority to act on behalf of the originator in respect of that data message; or

(b) by an information system programmed by, or on behalf of, the originator to operate automatically.

12.3. 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:

(a) 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

(b) 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.

12.4. Paragraph (3) does not apply:

(a) 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

(b) in a case within paragraph (3)(b), 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.

12.5. The addressee is entitle 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.

12.6. The addressee is not so entitled according to paragraph 5 when it knew or should have known that the transmission resulted in any error in the data message as received.

12.7. 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

13.1. Paragraphs (2) to (4) 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.

13.2. 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:

(a) any communication by the addressee, automated or otherwise, or
(b) any conduct of the addressee, sufficient to indicate to the originator that the data message has been received.

13.3. 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.

13.4. 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:

(a) 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

(b) if the received is not acknowledgement within the time specified in subparagraph (a), 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.

13.5. 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.

13.6. 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.

13.7. 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

14.1. 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.

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

(a) if the addressee has designated an information system for the purpose of receiving data messages, receipt occurs:

(i) at the time when the data message enters the designated information system; or

(ii) 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;

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

14.3. Paragraph (2) 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).

14.4. 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:

(a) 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;

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

PART TWO – ELECTRONIC COMMERCE IN SPECIFIC AREAS

Chapter IV
Carriage of Goods

Article 15
Actions Related to Contracts of Carriage of Goods

Without derogating from the provisions of part one of this Law, this chapter applies to any action in connection with, or in pursuance of, a contract of carriage of goods, including but not limited to:

a) furnishing the marks, number, quantity or weight of goods;
b) stating or declaring the nature or value of goods;
c) issuing a receipt for goods;
d) confirming that goods have been loaded;
e) notifying a person of terms and conditions of the contract;
f) giving instructions to a carrier;
g) claiming delivery of goods;
h) authorizing release of goods;
i) giving notice of loss of, or damage to, goods;
j) giving any other notice or statement in connection with the performance of the contract;
k) undertaking to deliver goods to a named person or a person authorized to claim delivery;
l) granting, acquiring, renouncing, surrendering, transferring or negotiating rights in goods;
m) acquiring or transferring rights and obligations under the contract.

Article 16
Transport Documents

16.1. Subject to paragraph (3), where the law requires that any action referred to in Article 15 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.

16.2. Paragraph (1) 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.

16.3. 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.

16.4. For the purposes of paragraph (3), 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.

16.5. Where one or more data messages are used to effect any action in subparagraphs (f) and (g) of Article 15, 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.

16.6. If a rule of 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.

PART THREE – INFORMATION SOCIETY SERVICES
Chapter V
Establishment and Information Requirements

Article 17
Establishment and Authorization

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

a) service providers utilizing their own infrastructure shall obtain authorizations pursuant to the applicable law on telecommunications (UNMIK Regulation 2003/16);

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

17.2. 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.

17.3. For the purposes of this definition in the previous paragraph (1):

a) “at a distance” means that the service is provided without the parties being simultaneously present;

b) “by electronic means” 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;

c) “at the individual request of a recipient of services”: means that the service is provided through the transmission of data on individual request.

17.4. This Law shall not apply to:

a) services not provided "at a distance";

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

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

   ii) consultation of an electronic catalogue in a shop with the customer on site; plane ticket reservation at a travel agency in the physical presence of the customer by means of a network of computers;

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

c) services not provided "by electronic means";

d) services having material content even though provided via electronic devices:

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

   ii) 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.

e) off-line services: distribution of CDROMs or software on diskettes;

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

   i) voice telephony services;
   ii) telefax/telex services;
   iii) services provided via voice telephony or fax;
   iv) telephone/telefax consultation of a doctor;
   v) telephone/telefax consultation of a lawyer;
   vi) telephone/telefax direct marketing.

g) services not supplied "at the individual request of a recipient of services";

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

i) radio broadcasting services;
ii) television broadcasting services;
iii) teletext provided by television broadcasters;
iv) all other broadcasting services as defined by the Telecom Law (UNMIK Regulation 2003/16).

Article 18
General Information to be provided by the Service Provider

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

a) the name of the service provider;

b) the geographic address at which the service provider is established;

c) the electronic mail address and universal record locator (URL) of the service provider;

d) the trade register in which the service provider is entered and his registration number (if applicable);

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

f) for regulated professions:

(i) any professional body or similar institution with which the service provider is registered;

(ii) the professional title and the jurisdiction where it has been granted;

(iii) a reference to the applicable professional rules in the jurisdiction of establishment and the means to access them;

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

18.2. 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 VI
Commercial Communications

Article 19
Information to be provided

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

a) the commercial communications need to be clearly identifiable as such;

b) the natural or legal person on whose behalf the commercial communication is made need to be clearly identifiable;

c) promotional offers (discounts, premiums and gifts) need to be clearly identifiable as such, including the conditions which are to be met to qualify for them;

d) promotional competitions or games, where permitted in the jurisdiction where the service provider is established, need to be clearly identifiable as such, including the conditions for participation.

Article 20
Unsolicited Commercial Communication

20.1. Unsolicited commercial communications by electronic mail are permitted provided however that such communications by a service provider need to be clearly identifiable and unambiguously as such.

20.2. Service providers should consult regularly and respect the opt-out registers in which natural persons not wishing to receive such commercial communications can register themselves.

Article 21
Regulated Professions

21.1. 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 independence, dignity and honour of the profession, professional secrecy and fairness towards clients and other members of the profession.

21.2. Professional bodies and associations are encouraged to establish codes of conduct which are fully compliant with European and international standards.

Chapter VII
Contracts Concluded by Electronic Means

Article 22
Information to be provided

22.1. Electronic contract means a contract concluded wholly or partly by electronic communications or wholly or partly in an electronic form

22.2. The following information is to be given 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:

a) the different technical steps to follow to conclude the contract;

b) whether or not the concluded contract will be filed by the service provider and whether it will be accessible;

c) the technical means for identifying and correcting input errors prior to the placing of the order;

d) the languages offered for the conclusion of the contract.

22.3. 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.

22.4. The provisions in paragraphs (2) and (3) do not apply to contracts concluded exclusively by exchange of electronic mail or individual communications.

22.5. 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 23
Placing of the Order

23.1. 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.

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

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

Chapter VIII
Liability of Intermediary Service Providers

Article 24
"Mere Conduit"

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:

a) does not initiate the transmission;
b) does not select the receiver of the transmission;
c) does not select or modify the information contained in the transmission.

Article 25
"Caching"

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, the service provider is not liable for the automatic, intermediate and temporary storage of that information, performed for the sole purpose of making more efficient the information's onward transmission to other recipients of the service upon their request, on condition that he:

a) does not modify the information;

b) complies with conditions on access to the information;

c) complies with rules regarding the updating of the information, specified in a manner widely recognized and used by industry;

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

e) acts expeditiously to remove or disable 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 disabled, or that a court or an administrative authority has ordered such removal or disablement.

Article 26
Hosting

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, on condition that he:

a) does not have actual knowledge of illegal activity or information and, as regards claims for damages, is not aware of facts or circumstances from which the illegal activity or information is apparent; or

b) upon obtaining such knowledge or awareness, acts expeditiously to remove or to disable access to the information.

Article 27
No General Obligation to Monitor

Information Society service providers, when providing the services covered by the Articles in this Chapter (Mere Conduit, Caching and Hosting), 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.

PART FOUR – DISTANCE CONTRACTS

Chapter IX
Definition and Scope

Article 28
Definition and Scope

28.1. For the purposes of this Law, a 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.

28.2. Distance communication include 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:

a) unaddressed printed matter;
b) addressed printed matter;
c) standard letter;
d) press advertising with order form;
e) catalogue;
f) telephone with human intervention;
g) telephone without human intervention (automatic calling machine or audio text);
h) radio;
i) videophone (telephone with screen);
j) videotext (microcomputer and television screen) with keyboard or touch screen;
k) electronic mail;
l) facsimile machine (fax);
m) television (teleshopping).

Article 29
Exemptions

29.1. This Law does not apply to contracts:

a) relating to any financial or insurance services will which the distance marketing of consumer financial services applies;

b) concluded by means of automatic vending machines or automated commercial premises;

c) concluded with telecommunications service providers through the use of public payphones;

d) concluded for the construction and sale of immovable property or relating to other immovable property rights, except for rental;

e) concluded at an auction.

29.2. The requirements related to Article 30, 31 , 32 and 33 do not apply to:

a) 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 roundsmen;

b) 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.

Chapter X
Process and Procedures
Article 30
Prior Information

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

a) the identity of the supplier and, in the case of contracts requiring payment in advance, his address;
b) the main characteristics of the goods and services;
c) the price of the goods or services including all taxes;
d) delivery costs, where appropriate;
e) the arrangements for payment, delivery or performance;
f) the existence of a right of withdrawal;
g) the cost of using the means of distance communication, where it is calculated other than at the basic rate;
h) the period for which the offer or the price remains valid;
i) 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.

30.2. All the above mentioned information, of which shall be related to the commercial transaction, needs to be provided in a clear and comprehensible manner. A due regard must be given to the principles of good faith in commercial transactions, and the principles governing the protection of those who are unable, pursuant to the applicable law, to give their consent, such as minors.

30.3. 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 31
Written Confirmation of Information

31.1. The consumer must receive written confirmation or confirmation in another durable medium available and accessible to him of the information mentioned in Article 30. This information must be provided at a reasonable time prior to the performance of the contract, and at the latest at the time of delivery, unless the information has already been given to the consumer prior to the conclusion of the contract in writing or on another durable medium.

31.2. In any event, the following must be provided:

a) written information on the conditions and procedures for exercising the right of withdrawal;

b) the geographical address of the place of business of the supplier to which the consumer may address any complaints;

c) information on after-sales services and guarantees which exist;

d) the conclusion for cancelling the contract, where it is of unspecified duration or a duration exceeding one (1) year.

31.3. 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 (1) 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 32
Right of Withdrawal

32.1. For any distance contract the consumer shall have a period of at least seven (7) working days in which to withdraw from the contract.

32.2. The only charge for the consumer because of the exercise of his right of withdrawal is the direct cost of returning the goods.

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

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

b) 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) month period referred to hereafter.

32.4. 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:

a) in the case of goods, from the day of receipt by the consumer;
b) in the case of services, from the day of conclusion of the contract.

32.5. If the mandatory written confirmation of information is supplied within this three (3) month period, the seven (7) working day period mentioned above will begin from that moment.

32.6. 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.

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

a) for the provision of services if performance has begun, with the consumer's agreement, before the end of the seven (7) working day period mentioned above;

b) 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;

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

d) for the supply of newspapers, periodicals and magazines;

e) for games and lottery services.

32.8. 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 33
Performance

33.1. 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.

33.2. Where a supplier fails to perform 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 in any case within thirty (30) days.

33.3. 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 35.

Article 34
Payment by Card

Consumers shall be entitled:

a) 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;

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

Article 35
Inertia Selling

Information Society service providers shall:

a) prohibit the supply of goods or services to a consumer without their being ordered by the consumer beforehand, where such supply involves a demand for payment;

b) exempt the consumer from the provision of any consideration in cases of unsolicited supply, the absence of a response not constituting consent.

Article 36
Restrictions on the use of Certain Means of Distance Communication

36.1. Use by the supplier of the following means requires the prior consent of the consumer:

a) automated calling system without human intervention (automatic calling machine);
b) facsimile machine (fax).

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

Article 37
Judicial or Administrative Redress

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:

a) public bodies or their representatives;
b) consumer organizations;
c) professional organizations.

Article 38
Binding Nature

The consumer may not waive the rights conferred on him by this Law. The consumer does not lose the protection granted by this Law by virtue of the choice of the law of a external jurisdiction as the law applicable to the contract if the latter has close connection with Kosovo or any Member State of the European Union.

PART FIVE – ELECTRONIC INVOICING

Article 39
Required Details on Invoices

39.1. The following details are required on invoices in electronic commerce:

a) the date of issue;

b) a sequential number, based on one or more series, which uniquely identifies the invoice;

c) the VAT identification number under which the taxable person supplied the goods or services;

d) the full name and address of the taxable person and of his customer;

e) the quantity, price, and nature of the goods supplied or the extent and nature of the services rendered;

f) 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;

g) 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;

h) the VAT rate applied;

i) the VAT amount payable.

39.2. It is not required that invoices be signed.

39.3. 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 40
Invoices on Paper or by Electronic Means

40.1. 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:

a) by means of an advanced electronic signature within the meaning of Article 2(2) of EU Directive 1999/93/EC; and

b) by means of an advanced electronic signature to be based on a qualified certificate and created by a secure-signature-creation device within the meaning of Article 2(6) and (10) of EU Directive 1999/93/EC; or

c) by means of electronic data interchange (EDI) as defined in Article 2 of European Commission Recommendation 1994/820/EC relating to the legal aspects of electronic data interchange when the agreement relating to the exchange provides for the use of procedures guaranteeing the authenticity of the origin and integrity of the data.

40.2. Invoices may be sent by other electronic means subject to the explicit acceptance by the consumer concerned.

40.3. 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 41
Storage of Invoices

41.1. 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 Code of Kosovo as established by the Ministry of Finance and Economy.

41.2. 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.

41.3. 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.

41.4. The Ministry of Finance and Economics 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.

41.5. Transmission and storage of invoices "by electronic means" 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.

PART SIX – ELECTRONIC PAYMENTS

Chapter XI
General Principles

Article 42
Objective

42.1. This Part of the Law 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:

a) for consumers, security and convenience;
b) for traders and issuers, greater security and productivity;
c) for the development of industry in Kosovo.

42.2. The principles of fair practice must be observed by all those who bring card payment systems into operation or make use of them.

42.3. 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.

Article 43
Contracts

43.1. Contracts concluded by issuers, or their agents, with traders and consumers 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.

43.2. Contracts shall be drawn up in the official language(s) of Kosovo as defined in the Constitutional Framework (UNMIK Regulation 2001/9).

43.3. 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.

43.4. All conditions, provided they are in conformity with the applicable law, shall be freely negotiable and clearly stipulated in the contract.

43.5. 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 44
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 45
Equipment

45.1. Electronic payment terminals shall register, control and transmit payments and may be integrated into a point-of-sale terminal.

45.2. Traders have the possibility, if they wish, to install a single or multi-card-terminal.

45.3. 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 46
Data Protection and Security

46.1. Electronic payments are irreversible. An order given by means of a payment card shall be irrevocable and may not be countermanded.

46.2. 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.

46.3. 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.

46.4. Contracts must not restrict trader's freedom of operation or freedom to compete.

Article 47
Fair Access to the System

47.1. Irrespective of their economic size, all service establishments concerned shall be allowed fair access to the system of electronic payment. A trader may be refused access only for reasons consistent with this Law.

47.2. 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.

Chapter XII
Supplementary Provisions
Article 48
Relations between Issuers and Traders

48.1. 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.

48.2. 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 49
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 50
Relations between Traders and Consumers

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

PART SEVEN – PROCESSING OF PERSONAL DATA AND PROTECTION OF PRIVACY

Chapter XIII
Protection of Individuals and Free Movement of Personal Data

Article 51
Principles of Protection of Personal Data Privacy

51.1. Information Society services shall be provided in Kosovo in accordance with the need to protect the fundamental rights and freedoms of natural persons and in particular their right to privacy with respect to the processing of personal data.

51.2. Notwithstanding this principle, service providers shall neither restrict nor prohibit the free flow of personal data inside or outside of Kosovo for reasons connected with the above mentioned protection.

51.3. This Law applies to the processing of personal data wholly or partly by automatic means, and to the processing otherwise than by automatic means of personal data which form part of a filing system or are intended to form part of such a system.

51.4. This Law does not apply to the processing of personal data in the course of an activity which falls outside the scope of the transferred powers, until they are transferred to the PISG. For example: processing operations concerning public emergency management, defense, security and the activities of UNMIK and the PISG in areas of criminal law. Neither does the Law apply to the processing of personal data by a natural person in the course of a purely personal or household activity.

Article 52
General Rules on the Lawfulness of the Processing of Personal Data

52.1. With respect to data quality, personal data shall be:

a) processed fairly and lawfully;
b) collected for specified, explicit and legitimate purposes
c) adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed;
d) accurate and, where necessary, kept up to date;
e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the data were collected or for which they are further processed.

52.2. In all cases in which personal data is collected, processed, stored or disseminated, the Information Society service provider shall establish a "controller" to ensure the compliance with paragraph (1) of this Article.

Article 53
Criteria for Making Data Processing Legitimate

Personal data shall be processed only if:

a) the data subject has given his consent; or

b) processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract; or

c) processing is necessary for compliance with a legal obligation to which the controller is subject; or

d) processing is necessary in order to protect the vital interests of the data subject; or

e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller or in a third party to whom the data are disclosed; or

f) processing is necessary for the purposes of the legitimate interests pursued by the controller or by the third party or parties to whom the data are disclosed, except where such interests are overridden by the interests for fundamental rights and freedoms of the data subject which require protection under Article 51 of this Law.

Article 54
Processing of Special Categories of Data

54.1. The processing of personal data shall be prohibited if it reveals:

a) racial or ethnic origin;
b) political opinions;
c) religious or philosophical beliefs;
d) trade-union membership;
e) health or sex life.

54.2. The restrictions imposed by paragraph (1) does not apply where:

a) the data subject has given his explicit consent to the processing of those data, except where the applicable laws of Kosovo provide that the prohibition referred to above may not be lifted by the data subject's giving his consent; or

b) processing is necessary for the purposes of carrying out the obligations and specific rights of the controller in the field of employment law in so far as it is authorized by the applicable law of Kosovo providing for adequate safeguards;

c) processing is necessary to protect the vital interests of the data subject or of another person where the data subject is physically or legally incapable of giving his consent; or

d) processing is carried out in the course in the course of its legitimate activities with appropriate guarantees by a foundation, association or any other non-profit seeking body with a political, philosophical, religious or trade-union aim and on condition that the processing relates solely to the members of the body or to persons who have regular contact with it in connection with its purposes and that the data are not disclosed to a third party without the consent of the data subjects; or

e) the processing relates to data which are manifestly made public by the data subject or is necessary for the establishment, exercise or defense of legal claims;

f) processing of the data is required for the purposes of preventive medicine, medical diagnosis, the provision of care or treatment or the management of health-care services, and where those data are processed by a health professional subject under national law or rules established by national competent bodies to the obligation of professional secrecy or by another person also subject to an equivalent obligation of secrecy.

Article 55
Information to be Given to the Data Subject

55.1. The controller or his representative must provide a data subject from whom data relating to himself are collected with at least the following information:

a) the identity of the controller and of his representative, if any;
b) the purposes of the processing for which the data are intended;
c) any information such as:

   (i) he recipients or categories of recipients of data;
   (ii) whether replies to the questions are obligatory or voluntary;
   (iii) the possible consequences of failure to reply;

d) the existence of the right of access to and right to rectify the data concerning him.

55.2. Where the data have not been obtained from the data subject, the controller or his representative must at the time of undertaking the recording of personal data or if a disclosure to a third party is envisaged, no later than the time when the data are first disclosed provide the data subject with at least the following information:

a) the identity of the controller and of his representative, if any;
b) the purposes of the processing;

c) any further information such as:

   (i) the categories of data concerned;
   (ii) the recipients or categories of recipients;

d) the existence of the right of access to and right to rectify the data concerning him.

Article 56
The Data Subject's Right of Access to Data

Every data subject has the right to obtain from the controller:

a) without constraint at reasonable intervals and without excessive delays or expense

b) confirmation as to whether or not data relating to him are being processed and information at least as to the purposes of the processing, the categories of data concerned, and the recipients or categories of recipients to whom the data are disclosed;

c) communication to him in an intelligible form of the data undergoing processing and of any available information as to their source;

d) knowledge of the logic involved in any automatic processing of data concerning him at least in the case of automated decisions;

e) as appropriate the rectification, erasing or blocking of data the processing of which does not comply with the provisions of this Law, in particular because of the incomplete or inaccurate nature of the data;

f) notification to third parties to whom the data have been disclosed of any rectification, erasure or blocking carried out in compliance with what has just been mentioned unless this proves impossible or involves a disproportionate effort.

Article 57
Exemptions and Restrictions

57.1. The mandatory obligations of this Law with respect to personal data and protection is without prejudice to the reserved powers of UNMIK, when such a restriction constitutes necessary measures to safeguard:

a) defense and public safety;

b) the prevention, investigation, detection and prosecution of criminal offenses, or of breaches of ethics for regulated professions;

c) an important economic or financial interest of UNMIK on behalf of Kosovo, including monetary, budgetary and taxation matters;

d) a monitoring, inspection or regulatory function connected, even occasionally, with the exercise of official authority in cases referred to in (b), (c) and (d);

e) the protection of the data subject or of the rights and freedoms of others.

57.2. Subject to adequate legal safeguards, in particular that the data are not used for taking measures or decision regarding any particular individual, data that is processed solely for purposes of scientific research or is kept in personal form for a period which does not exceed the period necessary for the sole purpose of creating statistics is exempted from the restrictions of this Chapter.

Article 58
The Data Subject's Right to Object

A data subject has the right:

a) in certain cases mentioned under Article 53 to object on compelling legitimate grounds relating to his particular situation to the processing of data relating to him, save where otherwise provided by applicable law;

b) to object to the processing of personal data relating to him which the controller anticipates being processed for the purposes of direct marketing, or to be informed before personal data are disclosed for the first time to third parties or used on their behalf for the purposes of direct marketing, and to be expressly offered the right to object free of charge to such disclosures or uses.

Article 59
Confidentiality and Security of Processing

59.1. Any person acting under the authority of the controller or of the processor, including the processor himself, who has access to personal data shall not process them except on instructions from the controller, unless he is required to do so by law.

59.2. The controller shall implement appropriate technical and organizational measures to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.

59.3. The carrying out of processing by way of a processor must be governed by a contract or legal act binding the processor to the controller and stipulating in particular that:

a) the processor shall act only on instructions from the controller;
b) the obligations set out in paragraph (2) shall also be incumbent on the processor.

Article 60
Obligation to Notify the Supervisory Authority

60.1. The controller or his representative, if any, must notify the supervisory authority referred to in Article 70 before carrying out any wholly or partly automatic processing operation or set of such operations intended to serve a single purpose or several related purposes.

60.2. The supervisory authority may provide for the simplification of or exemption from notification only in the following cases and under the following conditions:

a) where, for categories of processing operations which are unlikely, taking account of the data to be processed, to affect adversely the rights and freedoms of data subjects, they specify the purposes of the processing, the data or categories of data undergoing processing, the category or categories of data subject, the recipients or categories of recipient to whom the data are to be disclosed and the length of time the data are to be stored; and/or

b) where the controller, in compliance with the applicable law which governs him, appoints a personal data protection official, responsible in particular:

   (i) for ensuring in an independent manner the internal application of the applicable normative acts taken pursuant to this Law;
   (ii) for keeping the register of processing operations carried out by the controller, containing the items of information referred to in Article 20 (2) the Law,
   (iii) thereby ensuring that the rights and freedoms of the data subjects are unlikely to be adversely affected by the processing operations.

60.3. Paragraph (1) does not apply to processing whose sole purpose is the keeping of a register which according to applicable laws is intended to provide information to the public and which is open to consultation either by the public in general or by any person demonstrating a legitimate interest.

60.4. Certain or all non-automatic processing operations involving personal data shall be notified, or provide for these processing operations to be subject to simplified notification.

Article 61
Contents of Notification

61.1. The information to be given in the notification shall include at least:

a) the name and address of the controller and of his representative, if any;
b) the purpose or purposes of the processing;
c) a description of the category or categories of data subject and of the data or
d) categories of data relating to them;
e) the recipients or categories of recipient to whom the data might be disclosed;
f) proposed transfers of data to third countries;
g) a general description allowing a preliminary assessment to be made of the appropriateness of the measures taken pursuant to Article (16) to ensure security of processing.

61.2. The supervisory authority shall specify the procedures under which any change affecting the information referred to in paragraph (1) must be notified.

Article 62
Prior Checking

62.1. The supervisory authority shall determine the processing operations likely to present specific risks to the rights and freedoms of data subjects and shall check that these processing operations are examined prior to the start thereof.

62.2. Such prior checks shall be carried out by the supervisory authority following receipt of a notification from the controller or by the data protection official, who, in cases of doubt, must consult the supervisory authority.

62.3. The supervisory authority may carry out such checks in the context of preparation either as instructed by promulgated law or on subsequent normative acts, which define the nature of the processing and lay down appropriate safeguards.

Article 63
Publicizing of Processing Operations

63.1. The supervisory authority shall maintain a registry or summary of processing operations notified pursuant to Article 60. The register shall contain at least the information listed under Article 61. The register may be inspected by any person.

63.2. For processing operations not subject to notification, controllers or another body appointed by the Ministry of Transport and Communications shall make available at least the information referred to under Article 61 (first 5 items) in a reasonable summary form to any person on request.

63.3. This provision does not apply to processing whose sole purpose is the keeping of a register which according to applicable laws is intended to provide information to the public and which is open to consultation either by the public in general or by any person who can provide proof of a legitimate interest.

Chapter XIV
Appeal Procedure

Article 64
Remedies

64.1. Protection of rights determined to the present Law prior appeal to the Competent Court shall be guarantied to the first level by the Supervisory Authority referred to Article 70 of the present Law and to the second level by Telecommunications Regulatory Authority pursuant to UNMIK Regulation 2003/16.

64.2. Persons who considers any breach of his rights recognized by the present Law and not be satisfied with the services of provider is entitled to appeal to the Supervisory Authority obligated to solve out the complain in terms of 30 days since the day of receiving the complain.

64.3. Opposing the decision issued by the Supervisory Authority, a non satisfied person in terms of 15 days since the day when the decision was taken , is entitled to make appeal to the Telecommunications Regulatory Authority which is obligated to decide related to complain in terms of 30 days since the day of receiving the complain.

64.4. Decision of TRA related to complains may be contested to the competent Courts according to the Law on General Administrative Procedure into effect.

Article 65
Liability

65.1. Any person who has suffered damage as a result of an unlawful processing operation or of any act incompatible with this Law is entitled to receive compensation from the controller for the damage suffered.

65.2. The controller may be exempted from this liability, in whole or in part, if he proves that he is not responsible for the event giving rise to the damage.

Article 66
Sanctions

Sanctions to be imposed in the case of infringement of the provisions adopted pursuant to this Law shall be developed by the Competent Supervision Authority and have effect upon the written approval of the Ministry of Transport and Communications.

Chapter XV
Transfer of Personal Data to Third Countries

Article 67
Principles

67.1. The transfer to a third country of personal data which are undergoing processing or are intended for processing after transfer may take place only if, without prejudice to compliance with this Law, the third country in question ensures an adequate level of protection.

67.2. The adequacy of the level of protection afforded by a third country shall be assessed in the light of all the circumstances surrounding a data transfer operation or set of data transfer operations; particular consideration shall be given to the nature of the data, the purpose and duration of the proposed processing operation or operations, the country of origin and country of final destination, the rules of law, both general and sectoral, in force in the third country in question and the professional rules and security measures which are complied with in that country.

Article 68
Exceptions

68.1. With exemption of cases according to Article 67 save other data where otherwise provided by applicable law governing particular cases, transfers of personal data to a third country but does not ensure an adequate level of credibility within the meaning of Article 24 , on condition that:

a) the data subject has given his consent to the proposed transfer; or

b) the transfer is necessary for the performance of a contract between the data subject and the controller or the implementation of pre-contractual measures taken in response to the data subject's request; or

c) the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the controller and a third party; or

d) the transfer is necessary or legally required on important public interest grounds, or for the establishment, exercise or defense of legal claims; or

e) the transfer is necessary in order to protect the vital interests of the data subject; or

f) the transfer is made from a register which according to laws or regulations is intended to provide information to the public and which is open to consultation

either by the public in general or by any person who can demonstrate legitimate interest, to the extent that the conditions laid down in law for consultation are fulfilled in the particular case.

68.2. Without prejudice to paragraph (1), a transfer or a set of transfers of personal data to a third country which does not ensure an adequate level of protection may take place where the controller adduces adequate safeguards with respect to the protection of the privacy and fundamental rights and freedoms of individuals and as regards the exercise of the corresponding rights; such safeguards may in particular result from appropriate contractual clauses.

Article 69
Codes of Conduct

69.1. The Ministry of Transport and Communications may develop codes of conduct for the supervisory authority intended to contribute to the proper implementation of this Law, taking account of the specific features of the various sectors.

69.2. The Ministry may make provision for trade associations and other bodies representing other categories of controllers which have drawn up draft codes or which have the intention of amending or extending existing codes to be able to submit them to the implementation by the supervisory authority.

Article 70
Supervisory Authority on the Protection of Individuals with Regard to the Processing of Personal Data

70.1. The Ministry of Transport and Communications shall authorize one or more competent authorities to be responsible for monitoring the application of the provisions of this Law.

70.2. Supervisory authorities shall be consulted when drawing up administrative measures or regulations relating to the protection of individuals' rights and freedoms with regard to the processing of personal data.

70.3. Each supervisory authority shall in particular be endowed with:

a) investigative powers, such as powers of access to data forming the subject-matter of processing operations and powers to collect all the information necessary for the performance of its supervisory duties;

b) effective powers of intervention, such as, for example, that of delivering opinions before processing operations are carried out and ensuring appropriate publication of such opinions, of ordering the blocking, erasure or destruction of data, of imposing a temporary or definitive ban on processing, of warning or admonishing the controller, or that of referring the matter to national parliaments or other political institutions;

c) the power to engage in legal proceedings where the provisions adopted pursuant to this Law have been violated or to bring these violations to the attention of the judicial authorities.

70.4. Each supervisory authority hears claims lodged by any person, or by an association representing that person, concerning the protection of his rights and freedoms in regard to the processing of personal data. The person concerned shall be informed of the outcome of the claim.

Chapter XVI
Processing of Personal Data and the Protection of Privacy in the Electronic Communications Sector

Article 71
Scope and Coverage

71.1. This Law shall ensure an equivalent level of protection of fundamental rights and freedoms, and in particular the right to privacy, with respect to the processing of personal data in the electronic communication sector and to ensure the free movement of such data and of electronic communication equipment and services within and outside of Kosovo.

71.2. The provisions of this Law provides for the protection of the legitimate interests of subscribers who are legal persons.

71.3. This Law does not apply to activities concerning public security, defense, national security (including the economic well-being of Kosovo when the activities relate to security matters) and activities in the areas of criminal law.

Article 72
Services Concerned

72.1. This Law applies to the processing of personal data in connection with the provision of publicly available electronic communications services in public communications networks in Kosovo.

72.2. Articles 7, 9 and 10 shall apply to subscriber lines connected to digital exchanges and, where technically possible and if it does not require a disproportionate economic effort, to subscriber lines connected to analogue exchanges.

Article 73
Security

73.1. The provider of a publicly available electronic communications service shall take appropriate technical and organizational measures to safeguard security of its services . Having regard to the state of the art and the cost of their implementation, these measures shall ensure a level of security appropriate to the risk presented.

73.2. In case of a particular risk of a breach of the security of the network, the provider of a publicly available electronic communications service must inform the subscribers concerning such risk and, where the risk lies outside the scope of the measures to be taken by the service provider, of any possible remedies, including an indication of the likely costs involved.

Article 74
Confidentiality of Communications

74.1. The confidentiality of communications and the related traffic data by means of a public communications network and publicly available electronic communications services shall be preserved by the service provider. The service providers in particular shall prevent the eavesdropping, interfering to telephonic calls, saving or other overhearing or observation forms of communication and data circulation related to persons excluding the users, without the consent of the users concerned, except when legally authorized to do so. This does not prevent technical storage which is necessary for the conveyance of a communication without prejudice to the principle of confidentiality.

74.2. Paragraph (1) does not affect any legally authorized recording of communications and the related traffic data when carried out in the course of lawful business practice for the purpose of providing evidence of a commercial transaction or of any other business communication.

74.3. The use of electronic communications networks to store information or to gain access to information stored in the terminal equipment of a subscriber or user is only allowed on condition that the subscriber or user concerned is provided with clear and comprehensive information in accordance with European Directive 95/46/EC, inter alia about the purposes of the processing, and is offered the right to refuse such processing by the data controller. This shall not prevent any technical storage or access for the sole purpose of carrying out or facilitating the transmission of a communication over an electronic communications network, or as strictly necessary in order to provide an information society service explicitly requested by the subscriber or user.

Article 75
Traffic Data

75.1. Traffic data relating to subscribers and users processed and stored by the provider of a public communications network or publicly available electronic communications service must be erased or made anonymous when it is no longer needed for the purpose of the transmission of a communication.

75.2. Traffic data necessary for the purposes of subscriber billing and interconnection payments may be processed. Such processing is permissible only up to the end of the period during which the bill may lawfully be challenged or payment pursued.

75.3. For the purpose of marketing electronic communications services or for the provision of value added services, the provider of a publicly available electronic communications service may process the data referred to in paragraph (1) to the extent and for the duration necessary for such services or marketing, if the subscriber or user to whom the data relate has given his/her consent. Users or subscribers shall be given the possibility to withdraw their consent for the processing of traffic data at any time.

75.4. The service provider must inform the subscriber or user of the types of traffic data which are processed and of the duration of such processing for the purposes mentioned in paragraph (2) and, prior to obtaining consent, for the purposes mentioned in paragraph (3).

75.5. Processing of traffic data, in accordance with the preceding paragraphs in this Article, shall be restricted to persons acting under the authority of providers of the public

communications networks and publicly available electronic communications services handling billing or traffic management, customer enquiries, fraud detection, marketing electronic communications services or providing a value added service, and must be restricted to what is necessary for the purposes of such activities.

75.6. Paragraphs (1), (2), (3) and (5) shall apply without prejudice to the possibility for competent bodies to be informed of traffic data in conformity with applicable legislation with a view to settling disputes, in particular interconnection or billing disputes.

Article 76
Itemized Billing

Subscribers shall have the right to receive non-itemized bills. Service providers shall offer users the right to privacy of calling users and called subscribers, for example by ensuring that sufficient alternative privacy enhancing methods of communications or payments are available to such users and subscribers.

Article 77
Presentation and Restriction of Calling and Connected Line Identification

77.1. Where presentation of calling line identification is offered, the service provider must offer the calling user the possibility, using a simple means and free of charge, of preventing the presentation of the calling line identification on a per-call basis. The calling subscriber must have this possibility on a per-line basis.

77.2. Where presentation of calling line identification is offered, the service provider must offer the called subscriber the possibility, using a simple means and free of charge for reasonable use of this function, of preventing the presentation of the calling line identification of incoming calls.

77.3. Where presentation of calling line identification is offered and where the calling line identification is presented prior to the call being established, the service provider must offer the called subscriber the possibility, using a simple means, of rejecting incoming calls where the presentation of the calling line identification has been prevented by the calling user or subscriber.

77.4. Where presentation of connected line identification is offered, the service provider must offer the called subscriber the possibility, using a simple means and free of charge, of preventing the presentation of the connected line identification to the calling user.

77.5. Where presentation of calling and/or connected line identification is offered, the providers of publicly available electronic communications services shall inform the public thereof and of the possibilities set out in paragraphs (1), (2), (3) and (4).

Article 78
Location Data other than Traffic Data

78.1. Where location data other than traffic data, relating to users or subscribers of public communications networks or publicly available electronic communications services, can be processed, such data may only be processed when they are made anonymous, or with

the consent of the users or subscribers to the extent and for the duration necessary for the provision of a value added service.

78.2. The service provider shall inform the users or subscribers, prior to obtaining their consent, of the type of location data other than traffic data which will be processed, of the purposes and duration of the processing and whether the data will be transmitted to a third party for the purpose of providing the value added service.

78.3. Users or subscribers shall be given the possibility to withdraw their consent for the processing of location data other than traffic data at any time.

78.4. Where consent of the users or subscribers has been obtained for the processing of location data other than traffic data, the user or subscriber shall continue to have the possibility, using a simple means and free of charge, of temporarily refusing the processing of such data for each connection to the network or for each transmission of a communication.

78.5. Processing of location data other than traffic data in accordance with paragraphs (1) and (2),(3),(4) shall be restricted to persons acting under the authority of the provider of the public communications network or publicly available communications service or of the third party providing the value added service, and must be restricted to what is necessary for the purposes of providing the value added service.

Article 79
Exceptions

In specific cases, a provider of a public communications network and/or a publicly available electronic communications service may override the provisions of Articles 68 and 69:

a) the elimination of the presentation of calling line identification, on a temporary basis, upon the application of a subscriber requesting the tracing of malicious or nuisance calls. In this case, the data containing the identification of the calling subscriber will be stored and be made available by the provider of a public communications network and/or publicly available electronic communications service pursuant to UNMIK Regulation 2003/16.

b) the elimination of the presentation of calling line identification and the temporary denial or absence of consent of a subscriber or user for the processing of location data, on a per-line basis for organizations dealing with emergency calls and recognized as such by the applicable law in Kosovo, including law enforcement agencies, ambulance services and fire brigades, for the purpose of responding to such calls.

Article 80
Automatic Call Forwarding

Service providers shall ensure that any subscriber has the possibility, using a simple means and free of charge, of stopping automatic call forwarding by a third party to the user's terminal.

Article 81
Directories of Subscribers

81.1. Service providers shall ensure that subscribers are informed, free of charge and before they are included in the directory, about the purpose(s) of a printed or electronic directory of subscribers available to the public or obtainable through directory enquiry services, in which their personal data can be included and of any further usage possibilities based on search functions embedded in electronic versions of the directory.

81.2. Service providers shall ensure that subscribers are given the opportunity to determine whether their personal data are included in a public directory, and if so, which, to the extent that such data are relevant for the purpose of the directory as determined by the provider of the directory, and to verify, correct or withdraw such data. Not being included in a public subscriber directory, verifying, correcting or withdrawing personal data from it shall be free of charge.

81.3. Service providers may require that for any purpose of a public directory other than the search of contact details of persons on the basis of their name and, where necessary, a minimum of other identifiers, additional consent be asked of the subscribers.

81.4. Paragraphs (1) and (2) apply to all users.

Article 82
Unsolicited Communications

82.1. The use of automated calling systems without human intervention (automatic calling machines), facsimile machines (fax) or electronic mail for the purposes of direct marketing may only be allowed in respect of subscribers who have given their prior consent.

82.2. Notwithstanding paragraph (1), where a natural or legal person obtains from its customers their electronic contact details for electronic mail, in the context of the sale of a product or a service, in accordance with this law, the same natural or legal person may use these electronic contact details for direct marketing of its own similar products or services provided that customers clearly and distinctly are given the opportunity to object, free of charge and in an easy manner, to such use of electronic contact details when they are collected and on the occasion of each message in case the customer has not initially refused such use.

82.3. Service providers shall take appropriate measures to ensure that, free of charge, unsolicited communications for purposes of direct marketing, in cases other than those referred to in paragraphs (1) and (2), are not allowed either without the consent of the subscribers concerned or in respect of subscribers who do not wish to receive these communications.

82.4. The practice of sending electronic mail for purposes of direct marketing disguising or concealing the identity of the sender on whose behalf the communication is made, or without a valid address to which the recipient may send a request that such communications cease, shall be prohibited.

82.5. Paragraphs (1) and (3) shall apply to all users.

Article 83
Technical Features and Standardization

No mandatory requirements for specific technical features are imposed on terminal or other electronic communication equipment which could impede the placing of equipment on the market and the free circulation of such equipment within and outside of Kosovo.

PART EIGHT – ELECTRONIC SIGNATURES IN COMMERCE

Chapter XVII
General Provisions

Article 84
Purpose and Scope

This Law applies where electronic signatures are used in the context of commercial activities.

Article 85
Definitions

For the purposes of this Law:

"**Certificate**" means a data message or other record confirming the link between a signatory and signature creation data.

"**Certification service provider**" means a person that issues certificates and may provide other services related to electronic signatures pursuant to the Law.

"**Data message**" means 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;

"**Electronic signature**" means data in electronic form in, affixed to or logically associated with, a data message, which may be used to identify the signatory in relation to the data message and to indicate the signatory's approval of the information contained in the data message.

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

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

Article 86
Equal Treatment of Signature Technologies

Nothing in this Law, except Article 88, 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 Article 89 paragraph (1), or otherwise meets the requirements of applicable law.

Article 87
Interpretation

87.1. In the interpretation of this Law, regard is to be had to its international origin and to the need to promote uniformity in its application and the observance of good faith.

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

Article 88
Variation by Agreement

The provisions in Part eight of this 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 XVIII
Use of Signatures in Society

Article 89
Compliance with a Requirement for Signature

89.1. Where the law requires a signature of a person, that requirement is met in relation to a data message if an electronic signature is used that is as reliable as was appropriate for the purpose for which the data message was generated or communicated, in the light of all the circumstances, including any relevant agreement.

89.2. Paragraph (1) applies whether the requirement referred to therein is in the form of an obligation or whether the law simply provides consequences for the absence of a signature.

89.3. An electronic signature is considered to be reliable for the purpose of satisfying the requirement referred to in paragraph (1) if:

a) the signature creation data are, within the context in which they are used, linked to the signatory and to no other person;

b) the signature creation data were, at the time of signing, under the control of the signatory and of no other person;

c) any alteration to the electronic signature, made after the time of signing, is detectable; and

d) where a purpose of the legal requirement for a signature is to provide assurance as to the integrity of the information to which it relates, any alteration made to that information after the time of signing is detectable.

89.4. Paragraph (3) does not limit the ability of any person:

a) to establish in any other way, for the purpose of satisfying the requirement referred to in paragraph 1, the reliability of an electronic signature; or

b) to adduce evidence of the non-reliability of an electronic signature.

89.5. Unless specified otherwise in the applicable law, the provisions of this Article do not apply to the following:

a) land transactions;
b) divorces;
c) adoptions;
d) last will and testament.

Article 90
Practicability

90.1. The Commercial Court of Kosovo may determine which electronic signatures satisfy the provisions of Article 89 of this Law.

90.2. Any determination made under paragraph (1) shall be consistent with recognized international standards.

90.3. Nothing in this article affects the operation of the rules of private international law.

Article 91
Conduct of Signatory

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

a) exercise reasonable care to avoid unauthorized use of its signature creation data;

b) without undue delay, utilize means made available by the certification service provider pursuant to Article 92 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:

(i) the signatory knows that the signature creation data have been compromised; or

(ii) the circumstances known to the signatory give rise to a substantial risk that the signature creation data may have been compromised;

c) 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.

91.2. A signatory shall bear the legal consequences of its failure to satisfy the requirements of paragraph (1).

Article 92
Conduct of the Certification Service Provider

92.1. 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:

a) act in accordance with representations made by it with respect to its policies and practices;

b) 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;

c) provide reasonably accessible means that enable a relying party to ascertain from the certificate:

   (i) the identity of the certification service provider;
   (ii) that the signatory that is identified in the certificate had control of the signature creation data at the time when the certificate was issued;
   (iii) that signature creation data were valid at or before the time when the certificate was issued;

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

   (i) the method used to identify the signatory;
   (ii) any limitation on the purpose or value for which the signature creation data or the certificate may be used;
   (iii) that the signature creation data are valid and have not been compromised;
   (iv) any limitation on the scope or extent of liability stipulated by the certification service provider;
   (v) whether means exist for the signatory to give notice pursuant to Article 91, paragraph (1)(b), of this Law;
   (vi) whether a timely revocation service is offered;

e) where services under subparagraph (d) (v) are offered, provide a means for a signatory to give notice pursuant to Article 91, paragraph (1) (b), of this Law and, where services under subparagraph (d) (vi) are offered, ensure the availability of a timely revocation service;

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

92.2. A certification service provider shall bear the legal consequences of its failure to satisfy the requirements of paragraph (1).

Article 93
Trustworthiness

For the purposes of Article 92, paragraph (1) (f), 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:

a) financial and human resources, including existence of assets;

b) quality of hardware and software systems;

c) procedures for processing of certificates and applications for certificates and retention of records;

d) availability of information to signatories identified in certificates and to potential relying parties;

e) regularity and extent of audit by an independent body;

f) the existence of a declaration by the PISG, an accreditation body or the certification service provider regarding compliance with or existence of the foregoing; or

g) any other relevant factor.

Article 94
Conduct of the Relying Party

A relying party shall bear the legal consequences of its failure:

a) to take reasonable steps to verify the reliability of an electronic signature; or
b) where an electronic signature is supported by a certificate, to take reasonable steps:

(i) to verify the validity, suspension or revocation of the certificate; and
(ii) to observe any limitation with respect to the certificate.

Article 95
Recognition of Foreign Certificates and Electronic Signatures

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

a) to the geographic location where the certificate is issued or the electronic signature created or used; or

b) to the geographic location of the place of business of the issuer or signatory.

95.2. 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.

95.3. 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.

95.4. In determining whether a certificate or an electronic signature offers a substantially equivalent level of reliability for the purposes of paragraph (2) or (3), regard shall be had to recognized international standards and to any other relevant factors.

95.5. Where, notwithstanding paragraphs (2), (3) and (4), 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.

PART NINE – PROTECTION OF INFORMATION SYSTEMS

Chapter XIX
Information Systems in Society

Article 96
Scope and Purpose

The objective of this Part of the Law is 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 law in Kosovo in the area of attacks against Information Systems and data transfer.

Article 97
Definitions

For the purposes of this Law, the following definitions shall apply:

"**Authorized person**" means 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.

"**Computer**" means 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.

"**Computer data**" means any representation of facts, information or concepts which has been created or put into a form suitable for processing in an information system, including a program suitable for causing an information system to perform a function.

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

"**Electronic communications network**" means 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.

"**Information System**" means computers and electronic communication networks, as well as computer data stored, processed, retrieved or transmitted by them for the purposes of their operation, use, protection and maintenance.

"**Legal person**" means any entity having such status under the applicable law, except for States or other public bodies in the exercise of State authority and for public international organizations.

"**Without right**" means that conduct by authorized persons or other conduct recognized as lawful under domestic law is excluded.

Article 98
Illegal Access to Information Systems

98.1. 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:

a) against any part of an information system which is subject to specific protection measures; or
b) with the intent to cause damage to a natural or legal person; or
c) with the intent to result in an economic benefit.

98.2. The provisions of paragraph (1) specifically apply also to data interception.

Article 99
Illegal Interference with Information Systems

The following intentional conduct, without right, is punishable as a criminal offense:

a) 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;

b) 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.

Article 100
Instigation, Aiding, Abetting and Attempt

100.1. The intentional instigation of, aiding or abetting an offense referred to in Articles 98 and 99 is punishable.

100.2. Any attempt to commit the offenses referred to in Articles 98 and 99 is punishable.

Article 101
Penalties

101.1. Offenses referred to in Articles 98, 99 and 100 are punishable by penalties including a custodial sentence with a maximum term of imprisonment of no less than one (1) year in serious cases. Serious cases shall be understood as excluding cases where the conduct resulted in no damage or economic benefit.

101.2. The Commercial Court of Kosovo may impose fines in addition to or as an alternative to custodial sentences.

Article 102
Aggravating Circumstances

102.1. The offenses referred to in Articles 98, 99 and 100 are punishable by a custodial sentence with a maximum term of imprisonment of no less than four (4) years when they are committed under the following circumstances:

a) the 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;

b) the 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;

(c) the offense resulted in substantial proceeds.

102.2. The offenses referred to in Articles 98 and 100 are punishable by custodial sentences higher than those foreseen under Article 101, when the offender has been convicted of such an offense by a final judgment in the European Court of Justice.

Article 103
Particular Circumstances

Notwithstanding Articles 101 and 102, the penalties referred to in Articles 101 and 102 can be reduced, where, in the opinion of the competent judicial authority, the offender caused only minor damage.

Article 104
Liability of Legal Persons

104.1. Legal persons can be held liable for conducts referred to in Articles 98, 99 and 100, committed for their benefit by any person, acting either individually or as part of an organ of the legal person, who has a leading position within the legal person, based on:

a) a power of representation of the legal person, or
b) an authority to take decisions on behalf of the legal person, or
c) an authority to exercise control within the legal person.

104.2. Apart from the cases provided for in paragraph (1), a legal person can be held liable where the lack of supervision or control by a person referred to in paragraph 1 has made possible the commission of the offenses referred to in Articles 98, 99 and 100 for the benefit of that legal person by a person under its authority.

104.3. Liability of a legal person under paragraphs (1) and (2) shall not exclude criminal proceedings against natural persons who commit offenses or engage in the conduct referred to in Articles 98, 99 and 100.

Article 105
Sanctions on Legal Persons

105.1. A legal person held liable pursuant to Article 104 paragraph (1) is punishable by effective, proportionate and dissuasive sanctions, which shall include criminal or non-criminal fines and may include other sanctions, such as:

a) exclusion from entitlement to public benefits or aid;
b) temporary or permanent disqualification from the practice of commercial activities;
c) placing under judicial supervision; or
d) a judicial winding-up order.

105.2. A legal person held liable pursuant to Article 104 paragraph (2) is punishable by effective, proportionate and dissuasive sanctions or measures.

Article 106
Jurisdiction

106.1. The Commercial Court of Kosovo shall have the primary jurisdiction with regard to the offenses referred to in Articles 98, 99 and 100 where the offense has been committed:

a) in whole or in part, within Kosovo; or
b) by a resident of Kosovo and the action affects individuals or groups within Kosovo; or
c) for the benefit of a legal person that has its head office in Kosovo.

106.2. The jurisdiction established pursuant to paragraph (1) (a) shall include cases where:

a) the offender commits the offense when physically present in Kosovo, whether or not the offense is against an information system in Kosovo; or

b) the offense is against an information system in Kosovo, whether or not the offender commits the offense when physically present in Kosovo.

106.3. The SRSG has the final authority over the offenses referred to in Articles 98, 99 and 100 in cases where the Commercial Court of Kosovo refuses to hand over or extradite a person suspected or convicted of such an offense to a third country..

106.4. Where an offense falls within the jurisdiction of more than one country and when any of the jurisdictions concerned can validly prosecute on the basis of the same facts, the Commercial Court of Kosovo shall cooperate, in consultation with the SRSG, in order to decide which of them will prosecute the offenders with the aim, if possible, of centralizing proceedings in a single jurisdiction. To this end, the SRSG may have recourse to any body or mechanism established within the European Union in order to facilitate cooperation between their judicial authorities and the coordination of their action.

Article 107
Exchange of Information

For the purpose of exchange of information relating to the offenses referred to in Articles 98, 99 and 100, and in accordance with applicable law and data protection rules, the Commercial Court of Kosovo shall establish operational points of contact available twenty four hours a day and seven days a week.

Article 108
Implementation of the Law

The competent Authority can draw the Administrative Instruction for the implementation of this Law.

Article 109
Entry to the Force

The present law shall enter into force after adoption by the Assembly of Kosova on the date of its promulgation by the Special Representative of the Secretary-General.

Law No. 02/L-23
22 July 2005

President of the Assembly

Academic Nexhat Daci