Republika e Kosovës
Republika Kosovo - Republic of Kosovo
Kuvendi - Skupština - Assembly

Law No. 05/L -030

ON INTERCEPTION OF ELECTRONIC COMMUNICATIONS

Assembly of Republic of Kosovo,

Based on Article 65 (1) of Constitution of Republic of Kosovo,

Approves:

LAW ON INTERCEPTION OF ELECTRONIC COMMUNICATIONS

CHAPTER I
GENERAL PROVISIONS

Article 1
Purpose

1. This Law regulates the procedures and conditions for interception of electronic communications carried out for criminal procedure needs by state institutions established by law, and procedures and conditions of interception for security needs of the Republic of Kosovo and its citizens established by Law.

2. This Law determines the rules, obligations and procedures for Network Operators and Service Providers in relation to processing of certain data by them.

3. This Law determines the obligations and authorizations of state institutions established by law to safeguard the respect for human rights and freedoms in the process of lawful interception, as well as the oversight of the implementation of interception procedurës.

Article 2
Scope

This Law shall apply to all authorized institutions, competent authorities to order interception, network operators and to all Public Services Providers licensed by the Regulatory Authority of Electronic and Postal Communications, and other Institutions and Authorities defined and foreseen by this law.

Article 3
Definitions

1. The terms used in this Law shall have the following meaning:

1.1. **Call** - any fixed or temporary connection capable of transferring information between two or more users of the electronic communications system;

1.2. **Interception** - the legal activity of ensuring access and provision of an interception target's electronic communications and call associated data to an Authorized Institution pursuant to Chapter I or Chapter II of this Law;

1.3. **Interception of electronic communications** - the interception voice communications, textual communications or other communications through networks of fixed or mobile telephony. This includes any other similar tool or technological system that transmits data mainly intended to be private;

1.4. **Access** - the technical capability to interface with a communications centre in such a manner that an Authorized Institution, after the order for interception, can acquire and monitor communications and calls' related data carried out on that centre;

1.5. **Subject of interception** - one or more persons identified in a lawful authorization issued by the competent court pursuant to the Criminal Procedure Code and/or the Law on Kosovo Intelligence Agency, and whose incoming or outgoing communications are to be intercepted and monitored;

1.6. **Interception objects** - the signals, writings, images, audiovisual data or other type of information, to be obtained or transmitted through electronic communication equipment**;**

1.7. **Interception Interfaces -** the physical location of the technical equipment under the administration and control of the Chief State Prosecutor, as foreseen in Article 15 of this of this Law;

1.8. **Monitoring Centre** - the separate infrastructures of Kosovo Police and Kosovo Intelligence Agency as foreseen with Article 17 of this Law;

1.9. **Authorized Official -** the officer who is authorized, upon court order, to enforce all measures and means on interception set out with order on interception;

1.10.**Minimization upon judicial order** - a technical process by which the authorized official upon judicial order shall filter the data received during the interception which are not object of the investigation;

1.11. **Network Operator** - the lawfully licensed operator of a public electronic communications infrastructure, which permits the conveyance of signals between defined network termination points by wire, by microwave, by optical means or by electromagnetic means;

1.12. **Target Service** - a service associated with an interception target and usually specified in a lawful authorization for interception;

1.13. **Electronic Communication -** any transfer of signs, signals, of writings, images, sounds or data of other nature transmitted entirely or separately through systems of wire, radio, electromagnetic, photoelectric or photo-optic;

1.14. **Communication** - any information exchanged or conveyed between a certain numbers 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 this information;

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

1.16. **Service Provider** - the lawfully licensed legal person providing one or more public electronic communications services whose equipment consists wholly or partly in the transmission and routing of signals on an electronic communications network;

1.17. **Call-Associated data -** data signalling information passing between a target service and the network or another user. Includes signalling information used to establish the call and to control its progress (e.g. call on hold, call divert). Call-associated data also includes information about the call that is available to the network operator/service provider (e.g. duration of connection);

1.18. **RAEPC** - the Regulatory Authority of Electronic and Postal Communications;

1.19. **Data** - traffic data, location data and other necessary data to identify the subscriber or user;

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

1.21. **Telephone service** - calls (including voice, voicemail and video conference), supplementary services (including call forwarding and call transfer) and messaging or multi-media services (including short message services, enhanced media services and multimedia services);

1.22. **Lawful order** - the lawful order for interception issued pursuant with Chapter I and Chapter II of this Law;

1.23. **NAPPD** - the National Agency for Protection of Personal Data;

1.24. **KCPC** - the Kosovo Criminal Procedure Code;

1.25. **KIA** - the Kosovo Intelligence Agency;

1.26. **COECIP** - the Commissioner for Oversight of the Electronic Communications Interception Procedure;

1.27. **Short message services ("SMS")** - text message communication between electronic devices including, but not limited to, those of mobile phones, pagers and other mobile communication devices;

1.28. **For the purpose of this Law Meta-Data** shall mean all data related to communications that are subject to lawful interception order, including, inter alia, time, duration, source, destination, location and type of broadcast equipment or acceptance involved in communications, but excluding the content of a communication.

Article 4
Basic Principles of Interception

1. The basic guiding principles in case of interceptions pursuant to this Law are:

1.1. the respect for human rights and fundamental freedoms recognized and guaranteed by the Constitution and the European Convention on Human Rights and Freedoms, including the interpretation by the European Court of Human Rights through its judicial practice;

1.2. the prohibition of interception without a respective decision by the court. A lawful interception is considered only such interception for which a lawful order has been issued by the competent court to authorize interception.

2. In taking the decision for interception, the competent court is obliged to take into account:

2.1. the essence of rights and freedoms of persons for whom a request for interception has been made;

2.2. the significance and necessity for interception, and proportionality;

2.3. the nature, means and the extent of interception;

2.4. the relationship between the aim to be achieved and the possibility of achieving it through employing other investigative methods; and

2.5. secrecy and objectivity in the process of interception.

3. In taking the decision towards a request for interception and before authorizing interception as an investigative tool or for the collection of information, the competent court shall ensure that other investigative actions for the collection of information have been exhausted.

4. Based on the Constitution of Kosovo whereby freedom of expression and of the media are safeguarded, thus constituing a human rights standard in a democratic society, the competent court is obliged to respect and protect the journalists rights to protect the sources of information and not to disclose protected sources of information during the exercise of their functions as foreseen with the Law on the Protection of Journalism Sources and the Kosovo Criminal Code in the context of freedom of expression and information of the public as guaranteed by the European Convention on Human Rights and Freedoms and the judicial practice of the European Court of Human Rights on the protection of sources of journalists.

Article 5
Interception Types

1. For the purposes of this Law, the authorized institutions shall implement interceptions for the following needs:

1.1. Interception for the purpose of criminal procedure; and

1.2. Interception for the security needs of the Republic of Kosovo and its citizens.

Article 6
Procedure on Deciding for Interception

1. The procedure for lawful interceptions is implemented in three separate phases:

1.1. submission of requests for interception from institutions authorized by law;

1.2. review, approval and submission of requests for interception; and

1.3. court order for interception.

2. A lawful interception, for purposes of this law, shall be implemented only upon having gone through all three phases of the procedure in paragraph 1 of this Article.

Article 7
Limits on Interception

Competent authorities and authorized institutions to order interception are obliged to protect the rights of journalists to protect the sources of information and to prohibit the disclosure of protected source of information by persons participating as professionals (journalists) in publication of information or as member of media editorial board and his assistants foreseen with the Law on Protection of Journalism Sources, Criminal Code of Kosovo and the Constitution of Republic of Kosovo.

CHAPTER II
PROCEDURES AND CONDITIONS OF INTERCEPTION OF ELECTRONIC COMMUNICATIONS FOR PURPOSES OF CRIMINAL PROCEDURE

Article 8
Authorized Institutions to submit requests for lawful interception

1. For purposes of criminal procedure, the Kosovo State Prosecutor is the only authorized institution to submit request for lawful interception of electronic communications before the competent court.

2. The authorized institutions to propose a request before the Kosovo State Prosecutor for lawful interception for the purposes of criminal procedure are: Kosovo Police, Kosovo Customs, the Police Inspectorate of Kosovo, Kosovo Tax Administration, as well as the European Mission for the Rule of Law in Kosovo – EULEX, pursuant to its competencies delegated with the applicable legislation in the Republic of Kosovo.

3. The authorized institutions based on paragraph 2 of this Article shall exercise the authorizations from this Article only with the purpose of collecting the necessary data for carrying out their lawful duties.

4. Neither of the institutions foreseen with paragraph 1 and 2 of this Article has the right and authorizations to submit a request for interception for issues or actions which are not expressly provided by law and which are not within the scope of responsibilities and duties of such institutions.

Article 9
Request for Interception

1. The request for interception shall be drafted in sufficient copies, one copy of which is deposited with the Kosovo State Prosecutor and one is kept by the institution requesting the issuing of the Order for interception.

2. Except fulfilling the requirements of Articles 84-100 of Criminal Procedure Code of the Republic of Kosovo, a request of an authorized institution for lawful interception shall be in compliance with Article 4 of this Law and shall contain the following information:

2.1. the relevant data of the official person and his/her supervisor, and the functions of those who request the interception measures;

2.2. personal data and the address of the subject against whom the interception measures will be applied if such data is known;

2.3. the legal qualification of the measure and the clear legal basis for such measure;

2.4. the description of telecommunications which shall be intercepted for the purposes of criminal procedure and the data of the telecommunications operator which offers services to the subject to be intercepted;

2.5. detailed reasoning through which it is demonstrated that interception is necessary, as well as the reasoning that the data for which interception is requested cannot be collected by other investigative actions or for the collection of information;

2.6. time frame within which it is requested for the interception to take place.

Article 10
Competent authority to order interception measures in criminal procedure

1. The measure of electronic communications interception, including texts of messages or other electronic messages, interception of communications through computer networks shall be ordered only by the court upon the request of Kosovo State Prosecutor, except in cases when in

urgent criminal procedures it acts in accordance with the provisional order issued in writing pursuant to principles of this law.

2. In urgent criminal procedures, the competent authority to order in writing the provisional interception measure shall be the Kosovo State Prosecutor, in light of Article 91 of KCPC.

3. The provisional order from paragraph 2 of this Article shall cease its effects and any information or evidence collected during this period shall not be lawful if such order is not confirmed in writing from the competent Judge within three (3) days from the issuing of such order and provisional orders from paragraph 2 of this Article cannot be repeated.

4. The State Prosecutor is obliged according to official duty (ex officio) before issuing a provisional order to safeguard the respect of the basic principles foreseen in Article 4 of this Law.

Article 11
Order for Interception

1. The order for interception in criminal procedure shall be in conformity with Article 4 of this Law.

2. The order for interception measures shall not be issued for a period longer than sixty (60) days from the date of issuing of the order and can be extended only based on the criteria foreseen with the KCPC.

3. In addition to the requirements of KCPC, the order for interception shall contain the following information as well:

3.1. obligations for the office of the Kosovo State Prosecutor, Network Operators and/or Services Providers, as well as the Sector for Interception;

3.2. the institution that made the request;

3.3. the personal data and address of the subject of interception measures, if they are known;

3.4. number of protocol;

3.5. the time limit or deadline for interception, where the date and hour of start and finish are set;

3.6. operator of telecommunications that ensures communication;

3.7. end devices used by the subject of interception for the electronic communications; and

3.8. reasoning establishing that interception is necessary, as well as that the data for which interception is requested cannot be collected by other investigative or information collection actions.

4. During the implementation of the order for interception, the authorized official upon judicial order shall be obliged to minimize the interception according to the judicial order.

Article12
Obligations of Authorized Official

1. The authorized official for interception pursuant to this law is obliged to implement all measures and means foreseen with the Order for interception in such a way that it ensures authenticity, entirety and the security of data collected through interception.

2. The authorized official is obliged to ensure that no lawful interception is conducted without the Order for interception issued by the relevant court in accordance with Article 11 of this Law.

Article 13
Interception Sector within the Kosovo Police

1. The Interception Sector within the Kosovo Police carries out technical process of interception through monitoring center via telecommunication equipment for the interests of state institutions of law enforcement and investigation of criminal offences, based on the prior decision issued in accordance with this Law and KCPC.

2. The Lawful Interception Section shall ensure that interception Order contains all information required by Article 9 of this Law and execute only requests issued in full compliance with the provisions of this Law and the KCPC. If the request does not contain all the required data it shall be returned to the authorized official.

3. The Lawful Interception Sector registers the requests for interception and completes the acceptance/delivery form for the interception Order. The form of acceptance/delivery of interception Order shall contain: the type of Order or request, details from the Order for interception, the name of suspect, the information of the authorized officer requesting interception and his supervisor to implement the Order, authorized staff list to access the intercepted materials, evidence and other relevant materials for interception, identification document of the authorized officer or his delegate making the request.

4. Any request for interception is signed by the receiving officer and chief of the Interception Sector.

5. The Interception Sector shall be available through supervision twenty four (24) hours seven (7) days a week, and mainly in emergencies as required by the Criminal Procedure Code.

6. After the end of the received measure, the subject of the interception shall be notified in compliance with the provisions of the Criminal Procedure Code.

CHAPTER III
PROCEDURES AND REQUIREMENT OF INTERCEPTION OF ELECTRONIC COMMUNICATIONS FOR THE SECURITY NEEDS OF THE REPUBLIC OF KOSOVO AND ITS CITIZENS

Article 14
Procedures and Requirement of Interception of Electronic Communications for the Security Needs of the Republic of Kosovo and its citizens

Interceptions for the security needs of the Republic of Kosovo and its citizens are carried out in accordance with the Law on Kosovo Intelligence Agency, following the issuance of a Court Order from a Supreme Court judge, in accordance with Article 4 on the basic principles of interception set out by this Law.

Article 15
Interception System

1. Interception system is composed of two parts which cannot function independently from each other:

1.1. Interception Interface; and

1.2. Monitoring Center.

2. Production, market placing, sale or possession of electronic communications interception equipment, in the context of Article 15, paragraph 1 of this Law is allowed only when in compliance with applicable laws of Kosovo and is conducted in compliance with respective procedures by competent bodies, without obtaining a decision by the Government.

3. Areas where interception interface and monitoring center are installed shall guarantee full security of the information obtained through interception, including their monitoring and management system.

4. Each entry and exit in such areas shall be registered and supervised with a twenty four (24) hours supervision system, including tracing the identity of the official, recording the date and time of entry, information and activities conducted during this period of time, and length of stay inside, which ensures easy access, at later point in time, in relation to investigations on non-matching data or other verifications.

5. Such areas shall provide limited access in cases where an interception order is being applied.

Article16
Interception Interface

1. Interception Interface is a technical equipment which activates or ceases the interception of an end device upon Lawful Order for interception issued by the competent Court, under the administration and control of the Chief State Prosecutor.

2. Interception Interface shall possess a software and technical system that guarantees saving the complete traces of its use in compliance with this law.

3. Interception Interface shall maintain interceptions activation records. Such records are stored in accordance with the secondary legislation issued by the Prosecutorial Council, after consultation and agreement with the Agency for Personal Data Protection and Regulatory Authority of Electronic and Postal Communications, and is reported upon request to the Commissioner's attention in implementation of functions set out in Chapter V of this Law.

4. The authority administering the Interception interface reports solely to the Court and acts only based on lawful Court Order. Upon receipt of this Order, such authority enables and facilitates the interception process in technical aspect, in Monitoring Centres located in the Kosovo Police and the Kosovo Intelligence Agency.

5. Interception Interface cannot transmit intercepted communications to institutions or third parties except as provided in the Order authorizing the interception and in accordance with requirements of this Law.

6. Interception Interface shall be bound by the legal order and implement requested interception measures as soon as possible without unjustifiable delays.

Article 17
Parallel Interception

1. The Interception Interface shall have necessary technical and organizational capacity to implement multiple parallel interceptions for a single target at Monitoring Centre when this is requested from different Authorized Institutions, after a lawful Court Order of competent jurisdiction. In such cases, officials of the Interception Interface, Monitoring Centre, Network Operators, and Service Providers, undertake the necessary measures to protect the identity of the respective Authorized Institutions and to protect the confidentiality of the interceptions in accordance with this law.

2. Technical Standards in relation to parallel interceptions and maximum number of parallel interceptions shall be defined in secondary legislation, issued by RAEPC in accordance with

Chief State Prosecutor, which shall be in compliance with principles defined in Article 4 of this Law and the best European practices.

Article 18
Monitoring Centre

1. Monitoring Centre shall mean the separate infrastructure of authorized institutions in paragraph 2 of this Article, designed as destination of the transmission for intercepted communications and data related with of interception target call, and where the equipment for monitoring and recording is installed.

2. Monitoring Centres shall be installed at the Kosovo Police for interception of electronic communication under Chapter I of this Law for purposes of criminal procedures, which covers all authorized institutions with this law, and shall be installed at Kosovo Intelligence Agency for interception of electronic communications under Chapter II of this Law for the security needs of the Republic of Kosovo and its citizens. Monitoring units shall posses a software and technical system which guarantees saving all the traces of their use.

3. Persons in charge with certain function or duties on or in the process of interception are entirely or particularly prohibited to:

3.1. to disseminate or use the data collected outside the requirements of this law or the laws in force;

3.2. technical process of interception, entirely or particularly, constitutes classified information, the violation of which is punishable under the criminal legislation in force.

Article 19
Obligations of Network Operators

1. Each Network Operator is obligated to install the necessary infrastructure on their network, at its own expense, to ensure interception possibilities for their consumers that use their telecommunication services.

2. Infrastructure implemented by the telecommunications operators includes Interception Interface which secures interception abilities which needs to be in compliance with Monitoring Centres facilities.

3. Network operators are obliged to provide free of charge any service in function of interception process.

4. When network operators improve technologies, are obliged to cover with their costs the continuity of the functioning of the interception process.

Article 20
Principle of confidentiality of interceptions

1. Each lawful interception which is enabled by Interception Interface, Monitoring Centre, a Network Operator and Service Provider is conducted by respecting the principle of confidentiality and procedures established by this law, so that neither the interception target nor any other unauthorized person is aware of the interception.

2. No information about the targets of interception and methodology on how interception is conducted shall be reported or in any way be made available to the public or unauthorized persons, unless required by law.

3. Any data collected, retained or transmitted in connection with an interception must be protected so as to prevent and prohibit such unauthorized or unlawful use, and treat such data in accordance with standards of this law and other applicable laws.

Article 21
Safety of interception

1. Any person employed or contracted by the Interception Interface, Monitoring Centre and Network Operator for the installation, operation or maintenance of facilities, equipment, interfaces and interception software, including all employees who handle, or can be made aware, must have a security verification issued by the Kosovo Intelligence Agency in accordance with Law No. 03/L-178 for Classification of Information and Security Checks.

2. Objects, facilities, interfaces and softwares to be installed and used for interception purposes must have a verification issued by the Kosovo Intelligence Agency, certifying that they comply with technical and security requirements defined in secondary legislation issued by RAEPC.

Article 22
Oversight and penalties

1. After filing a written submission and reasoning by an authorized institution, the Regulatory Authority for Electronic and Postal Communications (The Authority) shall allow the Network Operator or Service Provider to take any necessary measures that are required to ensure compliance with this law and other applicable laws on interception and secondary legislation issued in accordance with these laws.

2. In case of disagreement by Network Operator or Service Provider with an order or decision issued in accordance with paragraph 1 of this Article, and violation of provisions defined in paragraphs 1 and 2 of Article 9 of this Law, the Authority in accordance with procedures for economic sanctions of the Law on Electronic Communications can punish Network Operator or respective Service Provider with a fine of eighty six thousand (86,000) Euro up to seven percent (7%) of annual revenues from activities related to electronic communications, taking into

account seriousness of refusal and its implications for the institutions of law enforcement and national security.

3. In case of repeated disagreement with orders or decisions issued in accordance with paragraphs 1 and 2 of this Article, the Authority may proceed with the issuance of the order to suspend the authorization of the Network Operator or respective Service Provider, until compliance with the order of the Authority is guaranteed.

4. In case of repeated disagreement with orders issued in accordance with paragraphs 1 and 2 of this Article that result or it is probable to result into a threat for the national security or that hamper seriously the operations of the institutions of Law and order enforcement, Authority may revoke licence/authorization of the respective Network Operator or Service Operator.

5. In order to exercise its powers under this Article, the Authority shall be authorized to enter and inspect the premises and operations of Network Operators or Service Providers during regular working hours and request from the Network operator or Service provider all information and documentation it deems necessary for the exercise of his authority under this Article.

Article 23
Destruction of Intercepted Data

After fulfilling the purpose and duties of authorized institutions and other relevant authorities within their competences and scope defined by law, the interception data must be destroyed in accordance with the obligations set out in the KCPC and the Law for the KIA.

CHAPTER IV
RETENTION AND DESTRUCTION OF DATA

Article 24
Types of data

The data referred to within this Chapter shall be the electronic data defined by the Law on Electronic Communications, and that relating to the Short Message Services.

Article 25
Data Storage

1. All data obtained through Lawful Interception shall be stored in a secure manner as required by the Criminal Procedure Code and the Law on the Kosovo Intelligence Agency.

2. Access to data obtained through lawful interception shall be strictly limited only to those individuals who are directly involved in the investigation of the matter to which the data relates and individuals required for the technical implementation of the Order for lawful interception.

3. Only data of direct relevance to a formal, on-going investigation may be retained.

Article 26
Retention and Destruction of data within the Monitoring Centre

1. The Chief State Prosecutor or his/her delegate shall ensure that any data obtained through lawful interception shall be retained only within the Monitoring Centre for as long as that information is relevant to an open investigation.

2. Any data obtained through lawful interception, and any duplicates, held within the Monitoring Centre shall be permanently erased and/or destroyed by the Chief State Prosecutor or his delegate within three (3) calendar months of it serving no useful investigative purpose.

3. The Chief State Prosecutor or their delegate will erase and/or destroy any remaining data that resulted from a lawful interception and which is retained within the Monitoring Centre no later than twelve (12) months after the conclusion of investigations.

Article 27
Retention and destruction of data within the interception facility of the Chief State Prosecutor ("CSP")

1. The Chief State Prosecutor or his delegate shall ensure that any personal data obtained through lawful interception shall only be retained within the CSP interception facility, as long as it is relevant to an open investigation.

2. Any data obtained through lawful interception, and any duplicates, shall be permanently erased and/or destroyed by the Chief State Prosecutor or his delegate within three (3) calendar months after it serving no useful investigative purpose.

3. The Chief State Prosecutor or his delegate shall delete and/or destroy any remaining date resulting from lawful interception, no later than twelve (12) months after the conclusion of investigations.

Article 28
Retention and destruction of data within the Kosovo Police interception facility

1. The Director of Kosovo Police or his delegate shall ensure that any personal data obtained through lawful interception shall only be retained within the Kosovo Police interception facility, as long as it is relevant to an open investigation.

2. Any data obtained through lawful interception and any duplicates, shall be permanently deleted and/or destroyed by the Director of the Kosovo Police or his delegate within three (3) calendar months after it serving no useful investigative purpose.

3. The Director of the Kosovo Police or their delegate shall erase and/or destroy any remaining date resulting from a lawful interception, no later than nine (9) months after the conclusion of investigations.

4. A Prosecutor, representing the Chief State Prosecutor shall personally monitor the destruction of abovementioned data by the Kosovo Police.

Article 29
Retention and destruction of data within the Kosovo Intelligence Agency interception facility

1. The Director of the Kosovo Intelligence Agency or his delegate shall ensure that any data obtained through lawful interception shall only be retained for as long as it is relevant to an ongoing investigation, and is directly related to the implementation of an Order from a Supreme Court judge.

2. Any data obtained through Lawful Interception and any duplicates, shall be permanently erased and/or destroyed by the Director of the Kosovo Intelligence Agency or their delegate within one (1) calendar month of it serving no useful investigative purpose relating to a Lawful Interception operation authorised by a Supreme Court Judge.

3. Except where a written waiver can be obtained from a Supreme Court Judge, the Director of the Kosovo Intelligence agency or his delegate will erase and/or destroy any remaining data that resulted from a lawful interception no later than nine (9) months after it was first intercepted.

4. The Inspector General of the Kosovo Intelligence Agency will monitor, in person, the destruction of the aforementioned data, by the Kosovo Intelligence Agency.

Article 30
Retention and Destruction of Data by the Network Operators and Service Providers

1. Network Operators and Service Providers shall not record, retain or duplicate any call or message content data.

2. Network Operators and Service Providers are permitted to retain meta-data for a maximum period of nine (9) calendar months, and shall make such data available to Authorized Institution in accordance with this Law for a period not exceeding nine (9) calendar months.

3. Following the expiry of the nine (9) calendar months period, the Network Operators shall the data shall erase and/or destroy the data and any duplicates.

4. Network Operators shall provide the Data Protection Agency and the Commissioner for the Control of Interception Legality with information about the quantity and type of interception data that they have destroyed on a six-monthly basis.

Article 31
Transitional period

1. Network Operators and Service Providers shall ensure procure, install, maintain and operate technical facilities, equipment, interfaces and software for the purpose of implementing Lawful Interception, and shall make any necessary organizational arrangements for the purpose of enabling Lawful Interception, as required by this Law, within six (6) month after the entry into force of this Law.

2. Call related data, including the contents of any communication, which has been collected and stored by Network Operators prior to the entry into force of this Law, shall continue to be retained by Network Operators and made available to Authorized Institutions in accordance with this Law for a period not exceeding nine (9) months. Following the expiry of the nine (9) months period, the data shall be destroyed in accordance with Article 13 of this Law.

3. A representative of the Data Protection Agency and the Commissioner for the Control of Interception Legality shall monitor, in person, the destruction of the data.

CHAPTER V
COMMISSIONER FOR OVERSIGHT OF INTERCEPTION PROCESS

Article 32
Oversight of interception

1. This Law hereby establishes the mechanism of Commissioner for Oversight of Interception of Communication (Commissioner).

2. Commissioner is a mechanism functioning within the institutional structure of the Kosovo Judicial Council, and conducts yearly control of the lawfulness of interception of communications in accordance with this Law, and reports to the Kosovo Judicial Council and to the State Prosecutor and respective parliamentary Committees of the Assembly of the Republic of Kosovo on annual basis on identified possible violations.

3. Commissioner is independent in exercising its functions and duties foreseen under this Law and has a separate budget within the annual operating budget of Kosovo Judicial Council, on the spending of which it reports to the Kosovo Judicial Council.

Article 33
Appointment of the Commissioner

The Commissioner is appointed by the Kosovo Judicial Council, from the group of judges of the Supreme Court. Commissioner is appointed for a term of 4 (four) years, and reports to the Kosovo Judicial Council and is subject to the principles defined by the Kosovo Judicial Council.

Article 34
Functions of the Commissioner

1. Commissioner exercises regular annual control on the lawfulness of the entire Interception process by the institutions authorized under this Law.

2. Annual control includes a detailed public report, preserving the confidentiality and purpose of the interception that analyses:

2.1. monitoring institutional coordination during implementation of interception of electronic communications based on the requirements of this Law, including potential violations, and drafting relevant recommendations;

2.2. comparison of interception traces in equipments inside “interception facilities” and “monitoring centre”, and decisions for lawful interception issued during that time period;

2.3. monitoring, based on selected samples, of legal standards of court decisions for lawful interception issued during that time period and promotion of unification of such standards within the Kosovo judicial system;

2.4. identification of violations of this Law in complying with procedures for implementation of lawful interception;

2.5. verification to check if authorized persons, within authorized institutions for lawful interception, have rightfully exercised their terms; and

2.6. verification of the destruction of information collected during the interception process, based on requirements of this Law, KCPC, and Law on Protection of Personal Data.

3. Conclusions and potential violations identified by the Commissioner have no legal effect in criminal procedures and decisions of competent courts. Conclusions issued by the Commissioner are reviewed by the Kosovo Judicial Council in cases related to interception for criminal

procedures, or General Inspector of KIA in cases related to lawful interception for the security needs of the Republic of Kosovo and its citizens.

4. In cases where violations are found, Kosovo Judicial Council addresses them to the Panel for Examination and Investigation based on Criminal Procedure Code, whereas the General Inspector addresses them based on competences under the Law on KIA.

5. The Commissioner shall inform the Agency for Protection of Personal Data with the findings of the report. The respective agency, in compliance with its legal competences shall take the actions it deems necessary to address the conclusions and findings from the commissioner's report.

6. In case of finding non-compliance and technical omissions referring to, but not only, the change of data between the data from the operators systems compared to the data from the interception traces in the equipments within the interception interface and monitoring centre, non-compliance, non-observance of order's time limits by the network operators or service providers, the Commissioner shall inform RAEPC with the findings of the report if such violation include actions from operators licensed by RAEPC. In case of finding such violation by the telecommunication operators, RAEPC addresses such violation pursuant to this Law and the Law on Electronic Communication with regard to its scope of competency.

7. The Commissioner has full access to institutions authorized to implement the decisions for lawful implementation and in the accompanying technical equipments which serve such a purpose.

8. The commissioner realizes the approach from paragraph 6 of this Article in the KIA premises in consultation, and upon authorization from the Inspector General of KIA.

9. The commissioner realizes the approach from paragraph 6 of this Article in the Kosovo Police premises in consultation with the General Director of Kosovo Police.

10. The Commissioner should cooperate closely with the Agency for the Protection of Personal Data on the protection of personal data and privacy.

11. The commissioner may not access the content of intercepted materials.

12. The conlusions of the Commissioner shall not influence in the individual appeal procedure before the National Agency for Protection of Personal Data (NAPPD).

Article 35
Technical support for the Commissioner

Kosovo Judicial Council shall regulate, through internal acts, the engagement of officials, technical support and other procedures required for exercising the term of the Commissioner at latest three (3) months after the entry into force of this Law.

CHAPTER VI
TRANSITIONAL PROVISIONS

Article 36
Transitional Provisions

1. Chief State Prosecutor within a period of six (6) months from the entry into force of this Law shall functionalize the interception interfaces, transitional infrastructure procedures, and human resources.

2. During this transition period, the Chief State Prosecutor shall be assisted by the Kosovo Police and Network Operators to functionalize the interception interface and ensuing procedures in technical and human resources aspect. Such assistance shall be financially supported by the Kosovo Prosecutorial Council.

3. Call related data and traffic, collected and retained in accordance with the Law upon a judicial order, by a network operator or service provider, shall be retained by the network operators and service providers for a period of nine (9) months after the entry into force of this Law.

4. The network operators and service providers should make available the data collected and retained according to paragraph 3 of this Article for a period of nine (9) months after the entry into force of this Law.

Article 37

Provisions of this Law shall prevail in case of conflict with the provisions of the Law on Electronic Communications.

Article 38
Entry into force

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

Law No.05/L-030
28 May 2015

President of the Assembly of the Republic of Kosovo

Kadri VESELI