

^LAW ON INTERCEPTION OF COMMUNICATIONS

I. GENERAL PROVISIONS

Article 1

This Law regulates the conditions and the procedure for interception of communications, the way of proceeding, keeping and usage of the received information and data with the application of this Law and the control of the legality of the interception of communications.

Article 2

No one is authorised to perform interception of communications without an order of the court of jurisdiction, except if it is intended for or there is an approval of the person or persons that are involved in the communication.

Article 3

The production, placing on the market, sales or holding of the means for interception of communications cannot be performed without an approval issued by the Ministry of Interior.

Article 4

The data collected by authorised interception of communications and the registries referring to them, have a characteristic of an official secret and are under special regime of protection, which is prescribed by the Minister of interior, i.e. the Minister of Defence in a Rulebook, the Minister of Justice with a court's rules of procedure and the Public Prosecutor of the Republic of Macedonia with instructions, each in their own activities.

The procedure for using, keeping and protection of data collected by authorised interception of communications is regulated with a special regime of protection referred to in paragraph 1 of this Article.

Article 5

The interception of communications is performed under conditions determined by this Law, in a way and in procedure that does not jeopardise human freedoms and rights which are not subject to limitation in accordance with this Law.

Interception of communications can last only a specific time, which is necessary for collecting data for realization of the purposes of interception, determined by this Law.

Article 6

The person whose communication was intercepted has the right to challenge the authenticity of the data collected and the legality of the procedure of interception of their communications, in a procedure determined by the Law on Criminal Procedure.

Article 7

Specific terms used in this Law have the following meaning:

- 1) Communication – each immediate conversation and each transfer of a human voice, of signs, signals, written text, pictures, sounds, data or information of any kind;
- 2) Interception of communications – secret acknowledging of the contents of any communication between people and creating a technical recording of the contents of the communication, with a possibility to copy it;
- 3) Means for interception of communications – electronic, mechanical or other means whose usage makes possible acknowledging or copying the content of any communication between people;
- 4) Telecommunication system – means, devices, instruments and medium of transfer;
- 5) Telecommunication service – each service that provides the users with the possibility of sending or receiving signs, signals, written text, pictures, sounds, data bases or information of any kind, fully or partially transferred through the telecommunication system;
- 6) Provider of telecommunication services – authorized legal person or few legal persons that provide services of the public telecommunication system or provide access to it, for the purpose of using it;
- 7) Authorised bodies for interception of communications – the Ministry of Interior and the Ministry of Defence and
- 8) Authorised officer – a person authorised by a decision of the Minister of Interior, i.e. the Minister of Defence to take over the activities in accordance with the provisions of this Law.

II. CONDITIONS AND PROCEDURE FOR INTERCEPTION OF COMMUNICATIONS FOR DETECTION AND PROSECUTION OF PERPETRATORS OF CRIMINAL ACTS

Article 8

The interception of communications of a certain person may be ordered by the court when there is reasonable doubt that the person is a perpetrator of a criminal act for which act a punishment of at least four years is prescribed, or a criminal act for which act a punishment of five years is prescribed there is a reasonable doubt that is being performed or is performed by an organised group, gang or another criminal association, for the purpose of providing data and evidence necessary for successful conducting of the criminal procedure which cannot be collected in another way.

Article 9

A request for establishing an order for interception of communications on the basis of Article 8 of this Law shall be submitted to the court by the Public Prosecutor in charge on their own initiative or on the proposal of the authorised officer by the Minister of Interior that is employed in the Ministry of Interior.

Article 10

The request for interception of communications shall be submitted to the investigative judge in charge in a written form and contains data on:

1. the body that submits the request for interception of communications;
2. data on the natural person or on the responsible person in the legal person whose communications are requested to be subject to interception;
3. reasonable doubt of a committed criminal act;
4. description of the criminal act;
5. the reasons for inability to collect the data and the evidence in another way;
6. the type of communications whose interception is requested;
7. the type of the possible technical means that should be applied and the possible locations of the means for interception of communications;
8. the manner and the scope of implementation of measures and
9. the time for which interception of communications is requested.

If it is necessary to enter in a home or in other premises or in transport means, for the purpose of installing, maintaining, using or removing the means for interception of communications, in the request referred to in paragraph 1 of this Article, it is stated as a different proposal, and for which the time period proposed for its performing should be specified.

Article 11

The investigative judge shall establish an order for interception of communications, 24 hours after the submittal of the request at latest, if on the basis of the facts and the circumstances listed in the request it is estimated that the data referred to in Article 10 of this Law are listed, the conditions referred to in Article 8 of this Law are met and are not contrary to the provisions of the Law on Criminal Procedure.

If the investigative judge does not agree with the request for establishing an order for interception of communications, the investigative judge will inform the Public Prosecutor in charge on the matter within 24 hours from the submittal of the request.

If the investigative judge does not agree with the request for establishing an order for interception of communications, the Public Prosecutor in charge has the right to an objection to the criminal council of the court in charge, within 24 hours from the notification on the disagreement.

The criminal council decides within 24 hours from the submittal of the objection.

Article 12

The investigative judge shall refuse the request for interception of communications if it refers to the communications of the lawyer assigned as a defender of the person whose communications are subject to interception, of the communications performed in the official premises of the President of the Assembly of the Republic of Macedonia, the President of the Republic of Macedonia, the President of the Government of the Republic of Macedonia and of the communications that are performed in the official premises of the Members of the Parliament of the Republic of Macedonia.

Article 13

The order on interception of communications contains data on:

1. the organ at whose request interception of communications is ordered;
2. the identity of the natural person or the responsible person in the legal person whose communications will be subject to interception, if they are known;
3. reasonable doubt for a committed criminal act;
4. legal qualification of a criminal act;
5. the reasons for inability to collect the data and evidence in another way;
6. type of communications which will be subject to interception;
7. type of the possible technical means which will be used and the location of the means for interception of communications;
8. the manner and scope of implementation of the measures;
9. the time for which interception of communications is allowed and
10. the term during which, after the performed interception of communications,

the data are delivered to the court.

The order referred to in paragraph 1 of this Article specifically determines that the interception of communications will cease even before the expiry of the time for which the following of communications is allowed when the expected information will be received.

The order on interception of communications, if necessary to enter a home or other premises or transport means for the purpose of setting up installation, maintenance, use or removal of means for interception of communications, details the time period in which this will be performed.

Article 14

In cases of emergency when there is danger of causing death or serious bodily injury of one or more persons or a material damage of property on a large scale, or when there is danger of escape of a person which is a perpetrator of a criminal act for which lifetime imprisonment is sentenced, interception of communications can be undertaken on the basis of an oral order of the investigative judge. The investigative judge prepares an official note for the issued oral order which is recorded in the court register.

The oral order of the investigative judge referred to in paragraph 1 of this Article is issued on oral request for interception on communications, for which the public prosecutor in charge prepares an official note.

For oral request on interception of communications the public prosecutor in charge is bound to immediately and within 3 hours at latest after the received oral order on interception of communications, to deliver a written request, pursuant to Article 10 of this Law.

If after the issued oral request a written request has not been issued pursuant to paragraph 3 of this Article, it will be deemed that the order on interception of communications has not been issued and the interception of communications is interrupted, which is noted by the judge in the official note referred to in paragraph 1 of this Article.

The collected data on interception of communications referred to in paragraph 4 of this Article are destroyed pursuant to Article 26 paragraph 2 of this Law.

Article 15

With the order on interception of communications the court will allow interception of communications for the necessary time, but no longer than 30 days from the day of its establishment.

After the expiry of the term referred to in paragraph 1 of this Article, the applicant is bound to inform the court in written form on the results of the interception of communications, and if necessary to extend it, to submit an additional proposal with a special explanation on the reasons for the extension of interception of communications.

On the basis of the additional proposal referred to in paragraph 2 of this Article, the investigative judge may establish an order for extension of interception on communications for another 90 days at most.

In the case of disagreement with the additional proposal on extension of interception of communications, the public prosecutor in charge is entitled to an objection pursuant to Article 11 paragraph 4 and 5 of this Law.

Article 16

The court immediately delivers the issued order on interception of communications to the public prosecutor in charge.

Article 17

The order referred to in Article 16 of this Law to the public prosecutor in charge, which with a decision determines an authorised officer in charge of carrying out the actions and means for interception of communications, laid down in the order.

Article 18

When the interception of communications is performed through a telecommunications system, the authorised officer referred to in Article 17 of this Law is bound to inform the person in charge in the provider of telecommunications services about the order.

The person in charge referred to in paragraph 1 of this Article is obliged to implement the measures and procedures determined in the order on interception of communications.

Implementing data from the court order on interception of communications at the provider of telecommunications services, the person in charge referred to in paragraph 1 of this Article is bound to keep them as official secret and to act according to the law.

The costs incurred with interception of communications through the telecommunications system are paid from budget funds of the Ministry of Interior, on the basis of a contract concluded between the Minister for Interior and the legal person performing telecommunications services.

If criminal procedure has been initiated against the person whose communications have been subject of interception, the paid funds referred to in paragraph 4 of this Article are considered to be costs of the procedure and are charged pursuant to the Law on Criminal Procedure.

Article 19

The authorised officer referred to in Article 17 of this Law is bound to apply all measures and means determined with the order on interception of communications, in a manner which provides authenticity, entirety and security of the data collected with interception of communications.

For the purpose of accomplishing the tasks referred to in paragraph 1 of this Article, the authorised officer is bound to enable secure registration and storage of the data collected with interception of communications by using technical means. The registration of the collected data is performed in source form, and the data are handled in accordance with the special regime determined in Article 4 of this Law.

Article 20

All data, files and other materials collected with implementation of the order on interception of communications are delivered to the court of jurisdiction within the term determined with the order on interception of communications.

The data referred to in paragraph 1 of this Article are stored in a special form of files, sealed by the judge who has ordered interception of communications.

Article 21

The court may order opening of the form of files if the evidence received in this way should be used in the criminal procedure before the court.

For every opening of the form of files the minutes should be made

Article 22

The investigative judge delivers the data received on the basis of the issued order to the public prosecutor in charge.

If the public prosecutor in charge does not submit a request for the instigation of an investigation within 30 days from the day of delivery of the data collected with interception of communications, the judge reaches a decision for their destruction.

The court may reach a decision for destruction of the data even in the case when he/she estimates that the collected data are insignificant for the procedure.

Before reaching the decision for destruction referred to in paragraph 1 or 2 of this Article, the court compulsorily obtains an opinion from the public prosecutor in charge, who is bound to deliver the opinion within 3 days from the day of delivery of the request.

Against the decision of the court for destruction of the data, the public prosecutor in charge is entitled to objection pursuant to Article 11 paragraph 4 and 5 of this Law.

Article 23

If the data collected with interception of communications, until reaching a decision for admissibility referred to in Article 25 of this Law or the destroyed data are published in public, the citizen who has suffered damage because of this is entitled to compensation for damage.

The means for compensation of damage referred to in paragraph 1 of this Article are provided from the budget of the Republic of Macedonia.

Article 24

After reaching a decision for conducting an investigation, the court summons the person whose communication has been intercepted to appear to court within 8 days for the purpose of getting acquainted with the material concerning interception of his/her communications.

In the case of paragraph 1 of this Article, the files from the form on interception of communications will not be presented for acquaintance with the defendant, as long as it does not make eligible the part that towards the opinion of the public prosecutor may:

1. jeopardise the nature and course of the investigation;
2. jeopardise the persons that have participated in any way in undertaking certain activities and actions concerning the interception of communications;
3. jeopardise the interests of other persons which are not involved in the actions.

Article 25

The court decides with a decision on the admissibility of the data received with interception of communications to be used as evidence in the criminal procedure.

Against the decision referred to in paragraph 1 of this Article the parties are entitled to appeal to the criminal council of the court of jurisdiction within 24 hours from its delivery.

The criminal court decides upon the appeal referred to in paragraph 2 of this Article within 48 hours from its delivery.

Article 26

After the effectiveness of the decision in the criminal procedure, which was conducted against a person whose communications were intercepted, the court reaches a special decision for destruction of the data within 15 days.

The destruction referred to in paragraph 1 of this Article is performed by the commission, composed of a judge, public prosecutor and a person authorised by the Minister for Interior.

Article 27

If during the interception of communications some data is discovered that is related to other criminal act, different of the one the interception is ordered for, but according to this Law it can be ordered interception of communications for, then these data may be used as evidence in a court criminal procedure, according to Article 25 of this Law.

Article 28

The person whose communication was intercepted contrary to the provisions of this Law may claim for indemnity.

The court that ordered interception of communications shall decide on the claim for indemnity referred to in paragraph 1 of this Article, in an emergency procedure which shall not last more than 3 months.

Against the court's decision of paragraph 2 of this Article the injured party has the right to appeal to a court of higher instance within 8 days of its reception. The court of higher instance shall decide on the appeal within 8 days of its submission.

The indemnity shall be charged to the Budget of the Republic of Macedonia.

III. CONDITIONS AND PROCEDURE FOR INTERCEPTION OF COMMUNICATIONS FOR PROTECTION OF COUNTRY'S SECURITY AND DEFENSE INTERESTS

Article 29

The court may order for interception of communications for a person for whom there is a reasonable doubt that is preparing to commit a criminal act against the state, armed forces or against humanity and international law.

Except in these cases, the court may order for interception of communications when an armed attack against the Republic of Macedonia is being prepared, incited, organized or participated in or its security system for performing its own functions is being disabled, if there is no other way to discover data for such activity in order to stop the commit of the criminal act, armed attack or disablement of the security system.

When during the interception of communications according to paragraphs 1 and 2 of this Article, it is acknowledged that the person is a perpetrator of a certain criminal act, than the procedure of interception of communications may continue according to the conditions of Article 8 of this Law and the previously collected data may be used according to the provisions of this Law.

Article 30

The Minister for Interior or a person authorized by him/her as well as the Minister for Defence or a person authorized by him/her may submit a request for establishing an order for interception of communications on the basis of Article 29 of this Law.

The request for interception of communications submitted in accordance with Article 29 paragraph 2 of this Law, besides the data of Article 10 of this Law has to contain a special explanation for the reasons the request is submitted for.

The request for interception of communications referred to in paragraph 1 of this Article shall be submitted to a judge of the Supreme Court of the Republic of Macedonia, appointed according to the Court's internal organisation.

Article 31

The judge of the Supreme Court shall establish an order for interception of communications within 24 hours of the request submission, if he/she estimates that, based on the facts and circumstances in the request, the conditions of Article 29 of this Law are fulfilled.

By exception of paragraph 1 of this Article and with a specially explained proposal for an emergency of the order issuance, the judge of the Supreme Court shall establish an order for interception of communications within 5 hours of the request submission.

If the judge does not approve the request for establishing an order for interception of communications, than he/she will notify the applicant thereof in a written form within 24 hours of the request submission.

In the case of emergency referred to in paragraph 2 of this Article, if the judge does not approve the request for establishing an order for interception of communications, he/she will notify the applicant thereof in a written form within 6 hours of the request submission.

If the judge does not approve the request for establishing an order for interception of communications, the applicant of the request may submit an objection to the Supreme Court within 24 hours from the notification for disapproval.

On the objection referred to in paragraph 5 of this Article, a Council of three judges of the Supreme Court whose member can not be the judge that decided on the request for establishing an order for interception of communications, shall decide, within 24 hours of its submission.

Article 32

In the procedure for interception of communications for protection of country's security and defence interests the provisions of Articles 10, 13, 14, 17, 18, 19 and 28 of this Law shall be applied appropriately. The authorisations the Minister for Interior has according to these articles shall also apply for the Minister for Defence in the case when the last is the applicant of the request for establishing an order for interception of communications.

Article 33

By establishing the order for interception of communications, the judge of the Supreme Court shall allow interception of communications for the time necessary, which can not be longer than 90 days.

After the expiry of the term referred to in paragraph 1 of this Article, on the basis of additional explanatory proposal, the judge may order the interception of communications to be extended for a year at most, including the time given with the first order.

In the case when the judge does not agree with the additional proposal for establishing an order for continuing the interception of communications, the applicant of the proposal may submit an objection to the Supreme Court within 24 hours from the notification for disapproval.

Following the objection referred to in paragraph 3 of this Article, Article 31 paragraph 6 of this Law shall be applied.

Article 34

The data for a person collected during the enforcement of the court order for interception of communications shall be kept in the Ministry of Interior i.e. Ministry of Defence under a special regime, for a period no longer than one year following the expiry of the term determined in the order.

Following the expiry of the term referred to in paragraph 1 of this article, the data and all materials about the enforcement of the order for interception of communications shall be destroyed under the surveillance of the judge who established the order and for their destruction minutes shall be made where only the number of the court order shall be registered. Simultaneously, all data for the person for whom the order was established shall be destroyed from the court register.

The minutes referred to in paragraph 2 of this article shall be made in two copies; one of each shall be given to the court and the applicant of the request for interception of communications.

IV. SURVEILLANCE AND CONTROL

Article 35

The surveillance over the enforcement of the measures taken over for interception of communications on behalf of the Ministry of Interior and the Ministry of Defence shall be carried out by the Assembly of the Republic of Macedonia.

Article 36

For the surveillance referred to in Article 35 of this Law the Assembly of the Republic of Macedonia shall establish a Committee composed of a president, four members, deputy president and four deputy members, all elected from among the Members of the Parliament of the Republic of Macedonia.

The President of the Committee referred to in paragraph 1 of this article is a member of the political party in opposition within the Assembly of the Republic of Macedonia which on the last parliamentary elections won most of the election votes, two members of the Committee are members of the governing political parties and two others are members of the political parties in opposition in the Assembly of the Republic of Macedonia.

Article 37

The mandate of the President and members of the Committee referred to in this Law shall last for four years.

Article 38

The Committee shall submit an annual report to the Assembly of the Republic of Macedonia on the surveillance over the legality of enforcing the measures carried out by the Ministry of Interior and the Ministry of Defence within 2 months following the end of the current year.

Article 39

The Committee adopts own Rules of procedure regulating issues on the procedure and manner of operation of the same Committee.

Article 40

The Ministry of Interior shall control the enforcement of the provision of Article 3 of this Law.

V. TRANSITIONAL AND FINAL PROVISIONS

Article 41

The state authorities and legal persons, who produce, offer for sale, sell or keep means for interception of communications shall adapt their work according to the provisions of this Law within 6 months from the date of entry into force of this Law.

Article 42

The Assembly of the Republic of Macedonia shall establish the Committee referred to in Article 36 of this Law within 60 days from the date of entry into force of this Law.

Article 43

The by-laws foreseen with this Law shall be adopted within three months from the date of entry into force of this Law.

Article 44

This Law shall enter into force on the eighth day from the day of its publication in the Official Gazette of the Republic of Macedonia.