

Republic of Macedonia

Constitutional Privacy Framework

The Constitution of the Republic of Macedonia¹ recognizes the rights of privacy, data protection and secrecy of communications. Article 25 states: "Each citizen is guaranteed the respect and protection of the privacy of his or her personal and family life and of his or her dignity and reputation. No one may interfere in the personal and family life, except in cases in which the expression and conduct of the person threatens the generally accepted social norms." Article 26 states: "(1) The inviolability of the home is guaranteed. (2) The right to the inviolability of the home may be restricted only by a court decision in cases of the detection or prevention of criminal offences or the protection of people's health. Article 18 states: "(1) The security and confidentiality of personal information are guaranteed. (2) Citizens are guaranteed protection from any violation of their personal integrity deriving from the registration of personal information through data processing." Equally guaranteed is the freedom and confidentiality of correspondence. Article 17 states: "(1) The freedom and confidentiality of correspondence and other forms of communication is guaranteed. (2) Only a court decision may authorize non-application of the principle of the inviolability of the confidentiality of correspondence and other forms of communication, in cases where it is indispensable to a criminal investigation or required in the interests of the defense of the Republic."

Data Protection Framework

Several laws regulate the right of privacy in the Republic of Macedonia. The Law on Personal Data Protection (LPDP) was adopted on January 25, 2005.² The LPDP explicitly identifies the exceptions from its application, focused on processing of personal data performed by natural persons purely for personal or household activities, processing of personal data in criminal procedure, as well as protection of the interests of security and defense of the Republic of Macedonia.³ According to the law, the personal data shall be processed fairly and lawfully, in conformity with the law and shall be collected for specified, explicit and legitimate purposes and shall be processed in a manner according to these purposes; they shall be adequate, relevant and not excessive in respect to the

1 Published in the Official Gazette of the Republic of Macedonia, Nos. 52/91, 01/92, 31/98, 91/01, 84/03. The Constitution is available at the website of the Constitutional Court <<http://www.usud.gov.mk>>, and the website of the President <<http://www.president.gov.mk>>.

2 No. 07/05.

3 LPDP at Article 4.

Macedonia

purposes they are collected or processed for.⁴ The data shall be accurate, complete and updated as needed. Inaccurate or incomplete data, having in mind the aims for which they were collected or processed, will be erased or rectified. The personal data shall be kept in a form that enables identification of the subject of personal data for not longer than it is necessary to fulfill the purposes for which the data were collected or for which they are further processed. The data controllers are responsible for complying with the abovementioned principles concerning the quality of personal data.⁵

The LPDP, in accordance with the Council of Europe (CoE) Convention No. 108, provides that consent of the data subject is mandatory for processing of personal data. Personal data can be processed without the consent of the subject if it is necessary for performance of a contract where the subject of personal data is a contracting party, or upon a request of the subject of personal data, prior to entering into a contract; for compliance with a legal obligation of the data controller; for protection of the vital interests of the subject of personal data; for performance of activities of public interest or of official authority vested in the data controller or a third party to whom the data were disclosed.⁶ Furthermore, the law prohibits processing of special categories of personal data. The LPDP stipulates that processing must be specially designated and protected, while transfer through a telecommunications network may be carried out if the data are specially protected with encryption methods to render them unreadable during transmission.⁷

The rights of the data subject include the right to examine the data collection; the right to submit a request to rectify, erase or block the processing of personal data, if the data are incomplete, inaccurate or out of date, or if their processing is not in conformity with the provisions of this law; and the right to request that their personal data are not used for advertising purposes.⁸ Furthermore, the LPDP guarantees that no court decision that produces legal effects concerning the performance of certain person can be based solely on automated data processing, the purpose of which is evaluation of certain personal aspects relating to that person.

The LPDP also established an obligation for data controllers to notify the Directorate for Protection of Personal Data before performing wholly or partly automatic processing operations and an obligation of the data controller to submit data on any newly opened collection of personal data, as well as any change of

⁴ *Id.* at Article 5.

⁵ *Id.* at Article 5, paragraph 2.

⁶ LPDP at Article 6.

⁷ *Id.* at Article 8.

⁸ *Id.* at Article 10.

data from the existing personal data collections.⁹ The records from the Central Register kept by the Directorate are publicly accessible, and they are published in the Official Gazette of the Republic of Macedonia.¹⁰ Additionally, transfer of personal data to other countries can be performed only if the third country provides an adequate level of protection of personal data.

Data controllers can make personal data available on the basis of a written request submitted by the user, if the data are needed to perform activities within the legally established scope of competences of the user. The LPDP stipulates a prohibition on providing personal data processing that cannot be carried out in accordance with the provisions of this law, and the purpose for requesting such personal data must be in accordance with specific, clear and lawful purposes for which personal data is collected.¹¹

In July 2008, the Parliament ratified the Additional Protocol of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data regarding supervisory authorities and trans-border data flow. This document was signed on January 4, 2008.¹² In July 2008, the Parliament also enacted the Law that amends the LPDP.¹³ Both pieces of legislation (the Additional Protocol and the amendments) came into force on August 19, 2008.¹⁴

The Law of amendments and modifications of the LPDP is aimed at:

- Full harmonization of the national legislation with the legislation of the European Union, more precisely with Directive 95/46/EC of the European Parliament and the Council of the European Union;

9Id. at Article 29, paragraph 1: "Data Controller is obligate to submit a report to the Directorate, containing data which is in accordance to the article 27 of the law, before performing wholly or partly automatic processing of personal data. Data Controller is obligate to report the Directorate for each change of the data from the existing personal data collections."

¹⁰ LPDP at Article 30.

¹¹ *Id.* at Article 34, paragraph 1 and 3: "(1) Data Controller can make personal data available on the basis of a written request submitted by the user, if the data are needed to perform activities within the legally established scope of competencies of the user. (3) Providing personal data whose processing, i.e. use cannot be carried out in accordance with the provisions of this Law is prohibited."

¹² „Указ за прогласување на Законот за ратификација на Дополнителниот протокол кон Конвенцијата за заштита на поединците во поглед на автоматска обработка на лични податоци во врска со надзорните тела и прекуграничниот пренос на“ (Decree for enacting the Law of Ratification of the Additional Protocol of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data regarding supervisory authorities and trans-order data flow) from the Official Gazette of Republic of Macedonia, August 19, 2008, republished on the website of Directorate for Personal Data Protection, available at

<http://dzlp.mk:8500/FILES/1164/PUBLIC/CONTENT/57980790416419030709141_FILES/CIJATA_ZA_ZA%5BITTA_NA_POEDINCITE_VO_POGLED_NA_AVTOMATS_KA_OBRABOTKA_NA_LI%5ENI_PODATOCI_VO_VRSKA_SO_NADZORNITE_TELA_I_PREKUGRANI%5ENIOT_PRENOS_NA_PODATOCL.pdf>

¹³ „Указ за прогласување на Законот за изменување и дополнување на Законот за заштита на лични податоци“ (“Decree for enacting the Law for changing and amending the Law on Personal Data Protection”) from the Official Gazette of Republic of Macedonia, August 19, 2008, republished on the website of Directorate for Personal Data Protection, available at

<http://dzlp.mk:8500/FILES/1164/PUBLIC/CONTENT/57980790416419030709141_FILES/ZAKON_ZA_IZMENUVAWE_I_DOPOLNUVAWE_NA_ZAKONOT_ZA_ZA%5BITTA_NA_LI%5ENI_PODATOCL.pdf>

¹⁴ Official Gazette of the Republic of Macedonia, No. 103.

Macedonia

- Full harmonization of the national legislation with the Additional Protocol to the CoE Convention 108/81;
- Expansion of the definition of “special categories of personal data” by adding philosophical beliefs, genetic data and biometric data;
- Full application of the Law to public security and criminal proceedings, as well as limited application to national security and defense;
- Partial exclusion of the application of the Law, when necessary for the purposes of professional journalism and artistic expression;
- Regulating video surveillance;
- Simplification of the notification procedure and complaints handling procedure;
- Regulating in greater detail the manner of performing inspections and increasing the competencies and enhancing the status of the inspectors;
- Harmonization of the Law on Personal Data Protection with the Law on Misdemeanors and strengthening the independence of the Directorate for Personal Data Protection.

The constitutional guarantee of protection of personal data is also regulated by the Criminal Code.¹⁵ The "abuse of personal data" is considered a crime under the Criminal Code. The punishment for this criminal offense consists of a prescribed fine or prison sentence of up to one year for the perpetrator who, contrary to conditions established by law and without the consent of the citizen, collects, processes or uses his personal data. The same fine is provided for any person breaks into computerized information systems of personal data with the intention to use the data for himself or herself or another person in order to gain benefit or to cause harm to another person. The criminal offense of "abuse of personal data" has an aggravated form if it is committed by officials carrying out their duty, and that punishment is a prison sentence of three months to three years. The attempt to commit such a crime is also punishable. With the new amendments of the Criminal Code in 2004, legal persons can also be perpetrators of the primary form of this crime and be punished with a fine.¹⁶

The Law on Organization and Operation of State Administrative Bodies¹⁷ provides that state administrative bodies do not disclose data related to national

15 Criminal Code, No. 37/96, 80/99, 4/02, 43/03 and 19/04, available online at <<http://www.mlrc.org.mk/law/CriminalCode.htm>>.

16 Criminal Code, Article 149: "(1) A person who collects, processes or uses personal data from a citizen without his permission, contrary to the conditions determined by law, shall be punished with a fine, or with imprisonment of up to one year. (2) The punishment from item 1 shall apply to a person who penetrates a computerized information system of personal data, with the intention of using them in order to attain some benefit for himself or for another, or to inflict some harm upon another. (3) If the crime from items 1 and 2 is committed by an official person while performing his duty, he shall be punished with imprisonment of three months to three years. (4) The attempt is punishable. (5) If the crime from item 1 is committed by a legal entity shall be punished with a fine."

17 Nos. 58/00 and 44/02.

security, official and business secrets, and personal data of citizens in accordance to the law that governs protection of personal data of citizens.

The Law on the Voter List¹⁸ protects the personal data collected in accordance with the LPDP and they must not be used for any purpose other than for exercising citizens' voting right in accordance with the Law on the Voter List. Any citizen may, within the period determined within this law, file a request for registering, amending or deleting data in the copies of the voter's list provided for public inspection in case they or any other citizen are not correctly registered on the list. Copies of the voter list, with data related to the ordinal number, surname, name, gender, date of birth and address, are provided to registered political parties and to independent candidates.¹⁹

The Law on Reporting Dwellings and Residence of Citizens²⁰ stipulates that the Ministry of the Interior provides protection from unauthorized access and use of the data contained in the records on the dwelling, change of home address and residence of the citizens.

The personal data on asylum seekers, recognized refugees and persons under humanitarian protection, as well as the data on their residence and the rights they enjoy in the Republic of Macedonia are contained in the Central Collection of Data, established, processed and used by the Ministry of the Interior (Asylum Section). The above collection of data is established, processed and used by the person handling the collection in accordance with the provisions of the LPDP. In accordance with the Law on Asylum and Temporary Protection,²¹ the data from the Central Collection of Data cannot be exchanged with the country of origin of the person to whom such data relates or with the country of origin of the members of his family.

The personal identification number of the citizen is a unique designation on the identification documents of the citizen. In accordance with the Law on Personal Identification Number,²² the Ministry of the Interior designates a personal identification number to the citizen according to the place of registration of the newborn child in the Registry of Births kept on the territory of the Republic of Macedonia. The Ministry of the Interior provides for the retention, use and protection of the data from unauthorized access in accordance with law.

18 Nos.42/02 and 35/04, available at <<http://faq.macedonia.org/politics/elections/law.on.voters.lists.html>>.

19 Law on Voter's List, Part III: "Protection of the personal data of the Voter's list," Article 28.

20 Nos. 36/92, 12/93 and 43/00.

21 No. 49/03.

22 No. 36/92.

Macedonia

Law enforcement officers, in accordance with the Code of Police Ethics,²³ are obliged to adhere to the citizens' right to privacy in accordance with the Constitution and the laws of the Republic of Macedonia. The collection, retention and use of personal data by the police is performed in accordance with law and the ratified international agreements for protecting personal data with appropriate restrictions and to the extent necessary for carrying out legal duties.

The Law on Classified Information²⁴ establishes the measures and activities for protecting classified information. The measures and activities for security of individuals, such as issuing a security certificate, are significant. The satisfaction of the conditions for issuing a security certificate is established through a security audit carried out upon previous written consent of the person to whom a security certificate is to be issued. The data from the completed security questionnaires are used for the purposes of the audit. The law comprises the NATO and EU standards on classified information.²⁵

The Law on State Statistics²⁶ regulates the protection of individual data (of natural or legal persons) collected and processed for statistical purposes. The individual data related to a legal or natural person, collected and processed for statistical purposes, are confidential data and as such can be used as separate data for statistical purposes only. By exception, access to such data is allowed for scientific purposes (without the identification data about the data subject). Publication or preparation of statistical data must be conducted in a form preventing the identification of the data subject, unless the data subject has agreed to such publishing. Data providers are notified of the data protection. The measures and techniques for protecting individual data collected and processed for statistical purposes are established in a Rulebook on the Measures and Techniques on the Protection of Individual Data Collected for Statistical Purposes (SSO internal document), adopted by the Director of the State Statistical Office. A Commission for Data Protection has been established within the above state administrative body to supervise the protection of data.²⁷

Illegal invasion of the privacy of communications is prohibited and punishable. In accordance with the Law on Electronic Communications, the holders, operators of telecommunication networks and means, as well as the providers of public telecommunication services are obliged to provide inviolability of

23 No. 03/04.

24 No. 9/04.

25 "Macedonian Parliament resumes 53rd session," February 10, 2005, MT. net News.

26 No. 54/97.

27 The website of State Statistical Office is available at <<http://www.stat.gov.mk/>>. According to the LPDP, Commission for Protection of Data is to be elected six months after the law goes into force, August 1, 2005. That is why the commission still does not have a homepage.

message confidentiality within their technical abilities.²⁸ Furthermore, the law contains provisions regulating protective measures for providing networks and services, communication confidentiality, caller or connecting line identification, and location information that is not traffic information, automatic call diverting, etc. The law provides privacy protection with prohibition of unauthorized wiretapping and data retention, lawful wiretapping, and prohibition of unrequested communication including telemarketing and spamming in compliance with EU standards (opt-in for inclusion in mailing lists, and the right to opt-out for users of existing mailing lists).²⁹ The Act creates an inspectorate within the Agency for Electronic Communications which stipulates monetary penalties of 4-7% of the annual income for legal entities and additional 327-410 Euros for the responsible individuals.³⁰ In April 2007, the Ministry of Transport and Communications initiated amendments to this Law which would increase the penalties for the offenders to EUR 1,500-8,000 for individual offenders.³¹ The changes in the Law on Personal Data Protection also tackle the issues of unwanted direct marketing, with fees of 500 Euros if the offender is an individual citizen, 2000 Euros for legal entities plus 700 Euros for the responsible executive.³²

A public panel on privacy in Macedonia held on August 26, 2008, as part of a public consultation to elaborate the Macedonia Report for Privacy and Human Rights Report 2008, reiterated the assertions from the previous year that there has been no public knowledge about cases of implementation of privacy protection provisions of the Law on Electronic Communications, and spamming remains widespread practice in the Macedonian business sector. Moreover, at least one company provides spamming services for other companies, and the number of Macedonian legal entities who have a privacy policy, (if any) remains insignificant.³³

The Law on the National Bank of the Republic of Macedonia obligates the members of the Council of the National Bank and the employees of the National Bank to keep official and business secrets.³⁴ This obligation binds these persons

28 No. 13/05 adopted on February 22, 2005.

29 No. 13/05 adopted on February 22, 2005.

30 Agency for Electronic Communications, available at <<http://www.aec.mk>>.

31 Filip Stojanovski, „Спамот е забранет во Македонија!“ [Spamming is prohibited in Macedonia], Razvigor [blog], May 218, 2007, available at <http://razvigormk.blogspot.com/2007/05/blog-post_18.html>. See also Vlado Apostolov „Имејл рекламите - бизнис или прекршок?“ [Commercials via e-mail – business or offense crime]”, Špic, June 11, 2007, available at

<<http://www.spic.com.mk/DesktopDefault.aspx?tabindex=5&tabid=1&EditionID=290&ArticleID=12514>>.

32 Natali N. Sotirovska, „За несаकани спам-пораки казни од 500 до 2.000 евра [Fees ranging from 500 to 2000 Euros for unwanted spam-messages], Dnevnik, August 29, 2008, available at

<<http://www.dnevnik.com.mk/?itemID=1FD6BF9F94C51940AA425A047194D9B5&arc=1>>.

33 “Debate on Privacy in Macedonia,” Metamorphosis Foundation website, September 29, 2008, available at <<http://www.metamorphosis.org.mk/content/view/1250/3/lang,en/>>.

34 Nos. 03/02, 51/03, 85/03 and 40/04.

Macedonia

for five years following the end of their membership in the Council of the National Bank. The data that are official or business secrets may be provided only upon written request of the court. Furthermore, the Banking Law³⁵ provides that banks should not reveal personal data that qualified as a business secret of the bank according to law, statute and other bank acts.³⁶ The obligation to keep a business secret, that persists after the termination of employment with the bank, also applies to persons with special rights and responsibilities, bank employees and other persons with access to bank operations. The data on savings and bank deposits of natural and legal entities, as well as data on the account operations of natural and legal persons, are business secrets of the bank. The above data may be provided only in the following cases: (1) If the client provides written consent to reveal the data; (2) Upon written request or order of the competent court; (3) Upon written request of the national bank for the purpose of supervision, or another body authorized by law; or (4) If the data are provided to the Directorate for Money Laundering Prevention, in accordance with law. Additionally, in accordance with the Law on Securities,³⁷ the management and the employees of the Central Securities Depository, as well as certified auditors, are obliged to keep the confidentiality of the data learned through their employment, unless they are obliged to provide such information in accordance with specified law.

Other regulations partially or indirectly regulate the right of privacy. The Law on Single Registry of the Population in the Republic of Macedonia³⁸ provides for the introduction, retention and contents of the single automated registry of the population in the Republic of Macedonia, the competent authority for keeping the registry, the protection of the data from the registry and the processing, publishing and use of the data from the registry.

The Law on Personal Identification Records of the Insured and Beneficiaries of Pension and Disability Insurance Rights³⁹ provides for protection of such records. This protection encompasses undertaking measures and activities for protecting the data from: unauthorized access, unauthorized processing, and prevention of destruction, loss, modification, abuse and unauthorized use of the data.

The Law on Keeping Labor Records⁴⁰ stipulates that the data contained in such records can be used for statistical purposes and for other official needs. Legally established data can also be used by individuals to whom the mentioned data refer to in order to exercise their rights.

35 Nos. 63/00, 103/00, 70/01, 37/02, 51/03, 85/03, 83/04.

36 *Id.*

37 Nos. 63/00, 103/00, 34/01, 04/02, 37/02, 31/03, 85/03 and 96/04.

38 Published in the Official Gazette of the SRM, No. 46/90.

39 Published in the Official Gazette of the Republic of Macedonia, No. 16/04.

40 No. 16/04.

The Law on Social Care⁴¹ provides an obligation for the social security institution and the employees to keep professional and official secrets. The Law protects the data and the facts discovered during procedures and decision-making concerning the rights of beneficiaries of social security, of legal family protection, and on the competencies established by criminal regulations.

Furthermore, the Law on Family⁴² establishes that the data on adoptions are an official secret. The Law on Health Care⁴³ specifies that health sector workers are obliged to take care of patients, to respect their dignity, to adhere to medical ethics and to keep professional secrets. The obligation to keep professional secrets refers to any worker who uses medical records or in any way (in performing their tasks) comes across data contained therein. In accordance with the Law on the Protection of the Population from Contagious Diseases,⁴⁴ the reporting of AIDS and the HIV infection, as well as microbiological findings for *Treponema pallidum*, *Neisseria gonorrhoeae*, congenital infections with the Rubella virus, *Toxoplasma gondii* and *Chlamydia gondii* is anonymous.

Data Protection Authority

The Directorate for the Protection of Personal Data, as an independent supervisory agency, was established in June 2005.⁴⁵ The LPDP provisions regulate the establishment of the Directorate as an independent and autonomous state body with the capacity of a legal entity. The Directorate is managed by a director who is appointed and dismissed by the Parliament of the Republic of Macedonia, upon nomination by the Government of the Republic of Macedonia. The Director is appointed for a five-year term, with the right to be re-elected a maximum of two times. The director and the deputy director of the Directorate are accountable to the Parliament of the Republic of Macedonia. The director and the employees of the Directorate must keep as official secrets the data that they have encountered in their work, both during the terms of office or employment within the Directorate and afterward. The employees of the Directorate have the status of civil servants. The work of the Directorate is fully funded by the Budget of the Republic of Macedonia. The Directorate is a separate beneficiary from the Budget.⁴⁶

41 No.50/97, 16/00, 17/03 and 65/04.

42 No. 80/92, 09/96, 38/04 and 83/04 – consolidated text.

43 No. 38/91, 46/93, 55/95, 17/97 – consolidated text and 10/04.

44 No. 66/04.

45 The office for Personal Data Protection Republic of Macedonia website, available at <<http://www.dzlp.mk/>>. See also <<http://www.cecprivacy.org/main.php?s=2&k=macedonia>>.

46 Email from Filip Stojanovski, *supra*.

Macedonia

From the establishment of the Directorate in June 2005 until the end of 2006, eleven new hirings of civil servants have been realized in accordance with the principle of fair participation of minorities. In 2007, three new hirings have been realized (one person was transferred), therefore the Directorate now has 15 employees and two elected officials. The capacity building program of the Directorate is planned to be completed by 2010 with 50 employees.⁴⁷

The Directorate has adopted all the necessary regulations for the implementation of the LPDP within the term of six months established by law, including implementation of a:

- Rulebook on the technical and organizational measures for secrecy and protection of Personal Data;
- Rulebook on the manner on record keeping, and the record form for Personal Data Collections;
- Rulebook on the form, contents and manner of administration of the Central Register;
- Rulebook on the Personal Data processing operations representing a special risk to the rights and freedoms of the Personal Data Subject;
- Rulebook on the format, contents and manner on records keeping for Transfer of Personal Data to other States.

Data controllers had two years (until December 19, 2007) to incorporate the LPDP regulations into their own business operations. The two-year period expired; therefore the penal provisions of the LPDP have entered into force.

The Directorate assesses the legality of the processing of personal data; publishes the principles of processing of personal data and ensures that the Data Controllers respect them; investigates and has access to the collections of personal data established by data controllers, according to type of subjects and aims; controls the operations for the processing of personal data that data controllers use; collects data necessary for the proper performance of its tasks; maintains a central register of collections of personal data; maintains records on the transfer of personal data to other countries; receives reports or complaints related to the processing of personal data by data controllers; issues prohibitions of further processing of personal data to data controllers; provides opinion on the secondary legislation of the Data Controllers; and performs other tasks established by law. The Directorate also provides expert opinions and interpretations in the area of personal data protection. For example, the Directorate issued recommendations for providers of social network services and users of social network services.⁴⁸

⁴⁷ Directorate of Data Protection in Macedonia, "Legal grounds for the protection of personal data in the national legislation," available at <<http://www.cecprivacy.org/main.php?s=2&k=macedonia>>.

⁴⁸ Metamorphosis, "Directorate makes recommendations on the use of social networking websites," available

For the period of 2007-2008, the Directorate gave priority in raising public awareness on the right of personal data protection. The Directorate implemented the Norwegian model on raising public awareness for youngsters in data protection.⁴⁹ The Directorate, in cooperation with the Metamorphosis Foundation and three secondary schools create educational content for the promotion of data protection at the school level.⁵⁰ As part of the promotion activities, scholars participated in a debate in which they discussed how to protect their personal data when they use the Internet and in every day situations.

The Central Register was created at the end of 2007. Citizens should have access to the Central Register via the Directorate website.⁵¹ The controllers who are obliged to notify their personal data filling systems to the Central Register (by December 19, 2007) will be allowed to do so automatically, once a system for their electronic identification has been set up.

If violations of the provisions of the LPDP are found in the course of processing of personal data, the data controller must, within 30 days from the date when the violations were detected: bring its work in line with the provisions of this law and remove the reasons that led to the violations; complete, update, correct, disclose or maintain the confidentiality of the personal data; adopt additional measures for protection of the collection of personal data; interrupt the transfer of personal data to other states; secure the data or their transfer to other entities; and erase the personal data. Upon decision of the director, an administrative dispute can be initiated.⁵²

According to the Directorate's report from October 2006 to June 2007, the most frequent violations of personal data based on citizens' complaints include: unlawful collection and processing of Personal Identification Numbers; unauthorized disclosure of personal data; processing of personal data on the Internet without subject' consent; identity theft; unlawful revelation of personal data to users and unauthorized transfer of personal data to other countries; and unauthorized recording and publication of photographs on the Internet.⁵³

LPDP specifies a transition period in which data controllers must fully adjust their operations to the Law within two years from the adoption of the by-laws (i.e. until December 19, 2007). During this transition period, the Directorate

at <<http://www.metamorphosis.org.mk/content/view/1182/lang,en/>>.

49 "You decide" (www.dubestemmer.no)

50 This project was done in the framework of the CRISP project, *hereinafter*:

51 <http://www.dzlp.mk/>

52 LPDP at Article 47, paragraphs 1 and 2.

53 Ivana Bilbilovska, "Everybody Collects Personal Data for PR Campaigns," *Vreme*, Feb. 7, 2007 available in English at <<http://www.metamorphosis.org.mk/content/view/871/4/lang,en/>>.

Macedonia

could not impose direct sanctions for the above mentioned breaches of the LPDP, so supervision interventions were mostly of educative and consultative character.

Wiretapping and Surveillance Rules

The Constitution of the Republic of Macedonia in Article 17 guarantees the freedom and confidentiality of correspondence and other forms of communication. In 2003, an amendment of this article was made in order to regulate wiretapping and other surveillance authorities. The new Article 17 provides for violation of the confidentiality of correspondence and other forms of communication only in cases where it is indispensable to prevent or to discover a crime, for a criminal investigation or required in the interests of the defense of the Republic. The search of homes and personal search and seizure are regulated in the Law on Criminal Procedure.⁵⁴ In general, a judge's warrant must be issued prior to such searches.

Even though wiretapping is regulated and unauthorized wiretapping is prohibited, the wiretapping cases initiated in the past have not reached closure in court. The most notable example is the process against the state initiated by 17 journalists who have been subject to surveillance in the "Big Ear" affair of 2001.⁵⁵ Over seven years, four different judges have unsuccessfully presided over this trial, and it was finally resolved at a retrial in June 2007. The state was found guilty, but the 17 plaintiffs stated that they remain dissatisfied with the compensation and the whole process.⁵⁶ Their representatives stated that they won't discontinue the trial already underway at the European Court of Human Rights in Strasbourg, based on their complaint.⁵⁷ The Appellate court has confirmed the verdict of the basic court, but has lowered the damage from the initial 6.000 Euros to approximately 4.000 Euros per journalist. The journalists have stated that "they are not satisfied with the compensation, and the precedent sets a signal that the violation of human rights is cheap in Macedonia."⁵⁸

In 2006, members of Parliament accused the government of conducting

54 Nos. 15/97, 74/04.

55 Natali N. Sotirovska. „Ново судење за „Големото уво““, [New Trial for the Great Ear,] Dnevnik, May 31, 2007, available at

<<http://www.dnevnik.com.mk/?itemID=FCB57A0DCE021A4087ACFA510B4BE394&arc=1>> (in Macedonian).

56 Each of the 17 wiretapped journalists received 6000 EUR in damages. „Прва пресуда за „Големото уво“, новинарите го добија процесот за прислушувањето“, [First Big Ear Sentence, the journalists win wiretapping process,] Utrinski vesnik, June 16, 2007, available at <

<<http://www.utrinski.com.mk/?ItemID=498D4220C6B47343B1ADB06695FFCFE6>> (in Macedonian).

57 Email from Filip Stojanovski, *supra*.

58 „Апелациониот суд потврди: Новинарите од Големото Уво биле прислукувани“ (“Appellate court confirms: The Big Ear Journalists were wiretapped”) Večer, September 2, 2008, available at <<http://www.vecer.com.mk/?ItemID=C50F895AE5A071478301A8CF24F47A51>>.

surveillance on over 1,400 individuals.⁵⁹ The executive and judiciary branch of the government have so far failed to provide adequate responses to statements by Members of Parliament dealing with wiretapping.⁶⁰

The Criminal Procedure Code (CPC) established special investigation measures.⁶¹ These measures ensure the gathering of evidence required for a successful criminal prosecution. These measures apply only when the evidence cannot be obtained in another manner or evidence-gathering is related to serious organized crimes.⁶²

The order for the application of special investigation measures⁶³ may be issued by the Public Prosecutor's Office, or by the Investigative Judge in the preliminary investigative procedure, or only by an Investigative Judge in the course of an investigative procedure.⁶⁴

According to Article 149, paragraph 2 of the CPC, the order should include: the name of the person against whom special investigation techniques will be applied (when the alleged perpetrator is known); the grounds to suspect that the crime has been committed; facts justifying the application of the special investigation techniques; as well as determination of the mode, scope and duration of application of the techniques. The CPC established that the evidence gathered with use of special investigation measures can be admissible only if the measures have been used and applied following the procedure set forth by law.

The application of the special investigation measures of communication interception is furthermore regulated by the Law on Communication Interception (LCI) which is the *lex specialis* in respect to the CPC and the application of these

59 Jasminka Dogova, "1.400 Persons Wiretapped?!", April 28, 2006, available at <<http://www.spic.com.mk/DesktopDefault.aspx?tabindex=1&tabid=1&EditionID=261&ArticleID=11821>> (in Macedonian).

60 Email from Filip Stojanovski, *supra*.

61 Published in the Official Gazette of the Republic of Macedonia No. 15/2005

62 *Supra*, Article 146.

63 According to Article 146 of the CPC special investigation measures are: 1) Communication interception and entry into the home and other premises or transportation vehicles for purposes of creating conditions for communication interception under conditions and in a procedure established by law; 2) Inspection of and search of a computer system, seizure of a computer system of parts thereof or the electronic database; 3) Secret surveillance, following, and visual-sound recording of persons and items using technical devices; 4) Simulated purchase of items and simulated giving bribe and simulated acceptance of a bribe; 5) Controlled delivery and transportation of persons and items; 6) Use of undercover agents for surveillance and gathering information or data; 7) Opening a simulated bank account at which criminal proceeds are to be deposited; and 8) Registering simulated legal entities or use of existing legal entities for purposes of gathering information.

64 Article 8 "Communication interception in respect of a person may be ordered in cases in which there are reasonable grounds to suspect that the person has committed a crime for which at least four year prison sentence has been prescribed or a crime for which a prison sentence of up to five years has been prescribed and in respect of which there are grounds to suspect that it has been perpetrated by an organized group, gang or other criminal association, for the purpose of ensuring information and evidence required for the successful criminal prosecution which cannot be otherwise gathered".

Macedonia

measures.⁶⁵ The application of the investigation measures envisaged in the LCI requires adoption of secondary legislation that would further specify the application of such measures.⁶⁶

The LCI also envisages the establishment of a Parliamentary Committee for the supervision of the application of communication interception techniques by the Ministry of the Interior and the Ministry of Defense. This Committee has been established *de facto* at the Parliament of the Republic of Macedonia, but it has not issued any report yet.

Computer and Cybercrime Related Provisions

Computer crimes are regulated by Article 251 of the Criminal Code.⁶⁷ This act was added to the Criminal Law in 1996. It is included in chapter 23, Criminal Acts against Property of the Republic of Macedonia.

Law enforcement professionals base their actions on the provisions of the LPDP and must obtain a court order (a warrant) in order to obtain information from private companies, such as internet providers (ISPs) or cybercafés. None of the major five ISPs displays a public copy of their privacy policy, and the Internet access or web hosting contracts do not include information about it or the rights of users according to the LPDP, or internal procedures and responsibilities for dealing with sensitive information.

Cybercafés operate under the Law for Entertainment Games and Games of Chance,⁶⁸ and are not required to implement additional standards in regard to protection of the privacy of the users. The only provision in that law related to privacy is the obligation of confidentiality in regard to winning or losing.⁶⁹ As a result, customers use the cybercafés at their own risk, and a number of cases of publishing excerpts of private conversations (IMs, IRC) suggest that many cafés retain activity logs and monitor the traffic in their establishments, without making that clear to their customers. Users are also threatened by other users, who take advantage of poor security in the cafés to install spyware and harvest data.

Very few Macedonian websites in general display privacy protection clauses explaining what type of data they gather from each visit and what they use it for.

⁶⁵ Published in the Official Gazette of the Republic of Macedonia No. 121/2006

⁶⁶ Article 42 of the LCI. The deadline envisaged in the LCI expired on February 22, 2007.

⁶⁷ Criminal Code, *supra*.

⁶⁸ Draft Law for Modification and Amendment to the Law on Games of Chance and Entertainment Games, Official Gazette of the Republic of Macedonia No 10/97 and 54/97.

⁶⁹ Law for Entertainment Games and Games of Chance at Article 82.

Such examples include the sites of ISPs (with one exception),⁷⁰ portals, media companies (all newspapers and TV stations), and state bodies (Government, President, Assembly, Ministries).

The government assigned a Minister in charge of Information Society Development, who announced creation of special laws on e-commerce and cybercrime. In contrast to similar policy efforts in the past—including the landmark National Strategy for Information Society Development (2004-2005) and the National Strategy for Electronic Communications and IT Development (January-April, 2007)—by end of May 2007 the task force working on these laws failed to include civil society representatives, and deadlines and progress of this initiative remain hidden from public view.⁷¹

Media Laws and Practice

According to representatives of both the regulatory Broadcasting Council of the Republic of Macedonia⁷² and the Association of Journalists in Macedonia,⁷³ media laws in Macedonia do not specifically address the protection of privacy. Article 62 of the Law on Broadcasting⁷⁴ includes provision of the right to response and correction if a medium publishes incorrect data, but includes no sanctions for revealing personal data.

Article 7 of the Code of Journalists of Macedonia,⁷⁵ adopted by the Association and enforced by the Council of Honor states: "The journalist shall respect the privacy of every person, except in cases when that is contrary to the public interest." Members of the association are "obliged to respect personal pain and grief," and must obtain the consent of a parent or guardian to interview or photograph children or persons "with special needs, who are not able to decide rationally."⁷⁶ Both above sources indicated that, to their knowledge, there were no complaints about any journalistic breach of privacy during the examined period, while there were numerous suits against journalists for slander and libel.

A search carried out using "Najdi," the Macedonian search engine⁷⁷ that indexes online news sources, provides an illustration of low media interest in the area of

70 MT.net uses the same privacy policy of its mother company, the Macedonian Telecom, which was developed for the purposes of landline telephony. (Personal inquiry with the staff of the legal department.)

71 Email from Filip Stojanovski, *supra*.

72 Broadcasting Council of the Republic of Macedonia website <<http://www.srd.org.mk>>.

73 Association of Journalists in Macedonia website <<http://www.znm.org.mk>>.

74 Published in the Official Gazette of the Republic of Macedonia, No.20/97 and 70/03.

75 Code of Journalists of Macedonia <<http://www.znm.org.mk/EN/code.asp>>.

76 *Id.* at Article 9.

77 Najdi! – the Macedonian search engine is available at <<http://najdi.org.mk>>.

Macedonia

privacy. The search⁷⁸ revealed 120 articles from June 1, 2004 to April 30, 2005 containing forms of the word "privacy" (keyword: *privatnost*, in Cyrillic), constituting 0.12% of the total of 96,808 pages from that period.

The following breakdown provides a rough illustration of the trends in the media. Namely, only 43% of the listed privacy-related articles referred to various forms of the actual notion of privacy in the country, while the rest were either referring to developments abroad (54%) or were irrelevant (horoscopes).

Of the articles dealing with privacy in Macedonia: 31% dealt with mutual accusations of politicians during election and referendum campaigns, and the issue of their right to stay away from the public eye; 27% dealt with the life of local celebrities, with the term "privacy" ("*privatnost*") often incorrectly used instead of "private life" ("*privaten zhivot*"); 21% referred to other privacy-related issues, such as search and seizure, sanctity of the home, privacy in health care and in public sector enterprises; 11% dealt with NGO activism; 8% discussed reactions to the new wiretapping law, and 2% included a review of anti-spyware software.

NGOs' Advocacy Work

There is no strong Macedonian human right NGO specialized in the protection of privacy and personal data protection. However, several NGOs cover the issue with specific focus in line with their missions and types of activities. Two matters were in particular subject of concern during the reported period: the protection of human rights of children on the Internet—including the privacy of children—and the protection of privacy by the police and law enforcement agencies.

The NGO Metamorphosis Foundation organizes an annual International Conference on Privacy Protection and Open Government, providing a forum for regional cooperation and networking of decision makers and activists from the Western Balkans with the purpose of Euro-integration, especially by continuous inclusion of EU-based European Digital Rights (EDRi) representatives as speakers and participants.⁷⁹ The Open Society Institute of Macedonia (FOSIM) advocates open government through public monitoring, educational and lobbying

⁷⁸ The URL for this particular search is

<http://najdi.org.mk/najdi?query=%EF%F0%E8%E2%E0%F2%ED%EE%F1%F2%2A&metaname=swishdefault&sort=timestamp&lat2cyr=on&dr_e_year=2005&dr_s_mon=6&dr_s_year=2004&dr_s_day=1&dr_e_day=30&dr_o=13&dr_e_mon=4&start=0>. Please note that the above results refer to search commenced June 1, 2005. Najdi! constantly updates its list of sources and results may vary as archives of new sites are indexed.

⁷⁹ Metamorphosis Foundation <<http://www.metamorphosis.org.mk>>; E-society Conference webpage <<http://www.e-society.org.mk>>. The E-society Conference is supported by OSCE and FOSIM; FOSIM <<http://www.soros.org.mk>>; European Digital Rights <<http://www.edri.org>>.

efforts aimed at promotion of the Law on Free Access to Information of Public Character, the LPDP and the Law on Classified Information in cooperation with the relevant state bodies and Metamorphosis.

On the occasion of International Data Protection Day, January 28, 2007, Metamorphosis and the Directorate, in cooperation with the EU project for Technical Assistance to the Establishment of the Directorate and Enforcement of the Data Protection Principles, prepared and published a special issue of the periodical Metamorphosis ICT Guide titled “Privacy as a Basic Human Right.” 500 printed copies have been distributed to government officials, MPs, media, and other stakeholders, including university students, free of charge, and the e-version of the Guide remains available for download on the Metamorphosis website.⁸⁰

The Metamorphosis Foundation initiated the Children’s Rights on the Internet – Safe and Protected (CRISP) project in 2007.⁸¹ The project involved the Directorate for Personal Data Protection of the Republic of Macedonia and a network of eleven NGOs working on the promotion and safeguarding of children's rights within their communities. CRISP is co-funded by the European Initiative for Democracy and Human Rights (EIDHR) and Metamorphosis. CRISP’s objective is to create educational content and skills on the protection of personal data within the Macedonian public education system.⁸² CRISP activities included the creation of educational content for children, parents and teachers as well as leaflets and posters in Macedonian and Albanian.

As of June 2008, the project activities covered 28 schools in the Yugoslav Republic of Macedonia, with the participation of 3,144 students, 411 teachers and 421 parents. The activities continue in September and October 2008, with the start of the new school year. The website received over 5,000 visits in the first 6 months of operation.

Legal experts and human rights activists have raised concerns about the extensive use of detention and violation of privacy and the presumption of innocence. The Macedonian Helsinki Committee⁸³ and the network of 5 local NGOs⁸⁴ that works with alleged victims of police abuse continuously condemned spectacular arrests by the police, which included inviting the media to film the handcuffed suspects escorted by law enforcement officers. In order to raise public awareness and

80 <<http://www.metamorphosis.org.mk/content/view/829/61/lang,en/>>.

81 Metamorphosis Foundation website <<http://www.metamorphosis.org.mk/>>.

82 CRISP project website is <<http://www.crisp.org.mk/>>, more information in English is included in the Case Study at the ePractice.EU portal <<http://www.epractice.eu/cases/crisp/>>.

83 More info on Helsinki Committee for Human Rights of the Republic of Macedonia can be found on their website <<http://www.mhc.org.mk/>> www.mhc.org.mk, including their very significant monthly reports.

84 The Human Rights Support Project’s activities and reactions can be found at <<http://www.hrsp.org.mk/>>.

Macedonia

condemn concrete violations and spectacular arrests, nine media events were organized. As a result, TV Telma, one of then six television stations with license for national coverage, adopted a policy to no longer broadcast any arrests and police-escorted transports.

Individual citizens have contributed to raising public awareness on privacy protection issues. The media showed significant attention to the public disclosure of the effects of 40-year state surveillance on the poet Jovan Koteski by the communist regime.⁸⁵ In addition, a number of Macedonian bloggers have also tackled privacy issues, in posts about information society development and politics on national level.⁸⁶

The Metamorphosis Foundation also provided opportunities for raising awareness of opinion and decision makers. For example, Metamorphosis Foundation included data protection sessions within the 2007 agenda of the Third International Conference e-Society.mk. This Conference served as a tool for the establishment of the eGovernment Western Balkans Network. The conference was also organized in Albania, Bosnia and Herzegovina, Croatia, Montenegro and Serbia, and included participation of EU-based experts, in particular members of EDRI.⁸⁷

In November 2007, the Recommendations for ICT Standards in the Civil Service in the Republic of Macedonia were published. The document stressed privacy, a key principle for eGovernment development.⁸⁸ The Government failed to provide any public response to these recommendations. However, during the June 2008 campaign, the leading political party announced that it will introduce IT-standards in the public institutions by 2010.⁸⁹

85 <<http://www.templum.com.mk/margina/sodrzina/margina71/jasna.htm>>.

86 The following URL by blog aggregator Najdi! presents a list of all articles from almost all Macedonian blogs which mention any form of the word privacy in Macedonian language

<http://najdi.org.mk/najdi?query=izvor%3Dblog+%EF%F0%E8%E2%E0%F2%ED%EE%F1%F2*&submit1=%CD%E0%BC%E4%E8%21&metaname=swishdefault&sort=timestamp&reverse=on>.

87 The project was supported by Foundation Open Society Institute – Macedonia (FOSIM) and the East-East program of the Open Society Institute (OSI).

88 Jovanovic, M., Janevski, Z., Jashari, B., Donevska, K., Ugrinoski, A., Kocovski, K., Stefanovski, A., Tasevski, G., Recommendations for ICT Standards in the Civil Service in the Republic of Macedonia (FOSIM, 2007), available at <http://gg.org.mk/pdf/recomendations_ICT.pdf>. Good Governance website is <<http://www.gg.org.mk>>.

89 “Program of VMRO-DPMNE for Rebirth 2008-2012: Rebirth in 100 steps, upgraded and expanded”, VMRO-DPMNE website, <<http://www.vmro-dpmne.org.mk/Dokumenti/Programa%202008%20EN%20WEB.pdf>>.

Open Government

Free access to information and the freedom of reception and transmission of information are guaranteed by the Macedonian Constitution.⁹⁰ After a drafting process of over four years, the Law on Free Access to Information of Public Character came into force on September 1, 2006.⁹¹ The Commission for Protection of the Right to Free Access to Public Information is in charge of monitoring of its implementation.⁹²

The Law on Local Self-Government of the Republic of Macedonia recognizes the obligation to support the public's right to information. Article 8 states: "(1) The organs of the municipality, the council committees, and public agencies established by the municipality shall be obliged to inform the citizens about their work, as well as about the plans and programs which are of importance for the development of the municipality without any compensation, in a way determined by the statute. (2) The municipality shall be obliged to enable access to the basic information about the services that it provides to its citizens, in a way and under conditions determined by the statute of the municipality."⁹³

In July 1999, the Republic of Macedonia signed and ratified the Convention on Access to Information, Public Participation in Decision-making and Access to Justice in Environmental Matters (Arhus Convention).⁹⁴

International Obligations

The Republic of Macedonia is a member of the Council of Europe and has signed and ratified the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data No. 108.⁹⁵ Furthermore, the Republic of Macedonia has signed and ratified the European Convention for the Protection of Human Rights and Fundamental Freedoms,⁹⁶ and in June 2004 ratified the CoE Convention on Cybercrime.⁹⁷ The LPDP is compatible and aligned with the standards and the criteria set forth by the European Parliament and the European Council Directive on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data 95/46/EC of 1995.

90 Article 16 of the Constitution

91 Law on Free Access to Information of Public Character, Official Gazette, #13. February 1, 2006.

92 <<http://www.sinf.gov.mk>>.

93 Published in the Official Gazette of the Republic of Macedonia, No.5/2002.

94 No.40/1999.

95 Published in the Official Gazette of the Republic of Macedonia, No. 07/05. Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS no.: 108).

96 Convention for the Protection of Human Rights and Fundamental Freedoms (ETS no.: 005).

97 Published in the Official Gazette of the Republic of Macedonia, No. 41/04. Convention on Cybercrime (ETS no.: 185).