Project implemented by Human Dynamics in association with:
IPS Institute
AlmavivA S.p.A.
Czech Office for Personal Data Protection OPDP
Privacy International

Project office:
Directorate for Personal Data Protection
ul.Samoilova nr.10, 1000 Skopje
Tel: (+389) 2 3230 635

Document 1.1.2 - 5

ANALYSIS OF THE NATIONAL ELECTRONIC COMMUNICATIONS LEGISLATION FROM THE ASPECT OF PERSONAL DATA PROTECTION

Component 1

Activity 1.1.2

The content of this report is the sole responsibility of Human Dynamics and can in no way be taken to reflect the views of the European Union

Support to the Directorate for Personal Data Protection

This project is funded by the European Union

Project implemented by Human Dynamics in association with:
IPS Institute
AlmavivA S.p.A.
Czech Office for Personal Data Protection OPDP
Privacy International

Project office:
Directorate for Personal Data Protection
ul.Samoilova nr.10, 1000 Skopje
Tel: (+389) 2 3230 635

Contents

Support to the Directorate for Personal Data Protection

This project is funded by the European Union

I. INTRODUCTION

1. BACKGROUND ON THE LEGISLATION IN THE AREA OF ELECTRONIC COMMUNICATIONS

Legislation in the field of electronic communications in the EU and worldwide has rather short history. Actually, it emerged in the late 20th century as a result of the intensive development of the telecommunication and information technologies. For a long period of time, the telecommunication market was not open to competition. Namely, telecommunications have been treated as area of public interest and operators that provided telecommunication services were state owned.

The privatisation of the state owned companies and liberalisation of this market began in the eighties. This process was accompanied by the fast and enormous progress of the technology, which all together caused development of new services in the field of electronic communications, such as mobile telephony, Internet, digital television. Therefore, term telecommunications became too narrow and it was replaced with the term electronic communications that encompasses all forms of infrastructure, services and equipment for data transmission. The term telecommunications is usually used to describe wire (cable) equipment and services for voice telephony, while the term electronic communications is much broader and includes other modern electronic means (optical, electromagnetic means) and services (Internet).

Regulatory framework for electronic communications, however comprehensive it may be, does not cover all the communication networks. Those of importance for the security, defence and intelligence are generally excluded from the application of these rules. Also, it does not apply to the terminal equipment and the content of the services provided.

2. EU REGULATORY FRAMEWORK ON ELECTRONIC COMMUNICATIONS

The current electronic communications regulatory framework package was adopted in 2002. It is comprised of several directives that, in general, cover all aspects of electronic communications. The following pieces of legislation were adopted in 2002:

1. Directive 2002/21/EC of the European Parliament and of the Council of 7 March 2002 on a common regulatory framework for electronic communications networks and services (Framework Directive) - *OJ L 108, 24.4.2002*

2. Directive 2002/20/EC of the European Parliament and of the Council of 7 March 2002 on the authorisation of electronic communications networks and services (Authorisation Directive) - *OJ L 108, 24.4.2002*

3. Directive 2002/19/EC of the European Parliament and of the Council of 7 March 2002 on access to, and interconnection of, electronic communications networks and associated facilities (Access Directive) - *OJ L 108, 24.4.2002*

4. Directive 2002/22/EC of the European Parliament and of the Council of 7 March 2002 on universal service and users' rights relating to electronic communications networks and services (Universal Service Directive) - *OJ L 108, 24.4.2002*

5. Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) – *OJ L 201, 31.07.2002*

6. Commission Directive 2002/77/EC of 16 September 2002 on competition in the markets for electronic communication networks and services (Liberalisation Consolidation) – *OJ L 249, 17.09.2002*

In the recent years, this package has been supplemented and/or amended with the following EU directives and regulations:

- **Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly**

available electronic communications services or of public communications networks and amending Directive 2002/58/EC

- Regulation (EC) No 717/2007 of the European Parliament and of the Council of 27 June 2007 on roaming on public mobile telephone networks within the Community and amending Directive 2002/21/EC - *OJ L 171, 29.6.2007*

- Regulation (EC) No 544/2009 of the European Parliament and of the Council of 18 June 2009 amending Regulation (EC) No 717/2007 on roaming on public mobile telephone networks within the Community and Directive 2002/21/EC on a common regulatory framework for electronic communications networks and services - *OJ L 167, 29.6.2009*

- Directive 2009/140/EC of the European Parliament and of the Council of 25 November 2009 amending Directives 2002/21/EC on a common regulatory framework for electronic communications networks and services, 2002/19/EC on access to, and interconnection of, electronic communications networks and associated facilities, and 2002/20/EC on the authorisation of electronic communications networks and services - *OJ L 337, 18.12.2009*

- **Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009 amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector and Regulation (EC) No 2006/2004 on cooperation between national authorities responsible for the enforcement of consumer protection laws – *OJ L 337, 18.12.2009***

- Regulation (EC) No. 1211/2009 of the European Parliament and of the Council of 25 November 2009 establishing the Body of European Regulators for Electronic Communications (BEREC) and the Office - *OJ L 337, 18.12.2009*

As far as the personal data processing concerns, three pieces of afore-mentioned legislation regulate this aspect (written in bold): Directive 2002/58/EC on privacy and electronic communications, Directive 2006/24/EC and Directive 2009/136/EC, the latter two amending and/or supplementing the first one. The specifics and the importance of the personal data in this field was the main reason why EU legislators have decided to regulate this aspect in a separate Directive. However, it should be

noted that still the basic rules relating to personal data protection, which apply to this sector as well, are given in the *Directive 95/64/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data [OJ L 281/31 of 23.11.1995].* These sector specific directives regulate the specifics of data processing in electronic communications in order to protect fundamental rights and freedoms of natural persons, in particular with regard to the increasing capacity for automated storage and processing of data relating to subscribers and users.

3. ELECTRONIC COMMUNICATIONS REGULATORY FRAMEWORK OF THE COUNTRY

Law on Electronic Communications was adopted in 2005. Since then, it has been amended four times. It is the first comprehensive law that regulates the electronic communications. The Law has been harmonized with the EU regulatory framework on electronic communications, thus making the long-awaited liberalization in all segments of this market possible. In addition to this Law, the Government, the Ministry of Transport and Communication and/or the Agency for Electronic Communications (hereinafter: AEC or Agency) have adopted over 30 bylaws, each regulating a specific segment of the electronic communications. List of electronic communication legislation relevant for this analysis (laws and bylaws that contain personal data related provisions) is given in Chapter 2 of this document, while the content of these provisions and notes on their meaning and compliance with the legislation on personal data protection is given in Chapter 3.

4. USEFUL PRACTICAL INFORMATION RELATING TO DATA CONTROLLERS IN THIS SECTOR

National legislation in the field of electronic communications applies to numerous operators and service providers. They all collect and/or process data on their clients (subscribers), who may be legal and physical persons. Therefore, according to the Law on Personal Data Protection (hereinafter: LPDP), these operators and service providers are considered to be data controllers. This

means that they need to follow and implement the personal data protection rules set in LPDP and the bylaws based on this law, but also personal data protection provisions laid down in the electronic communications laws and bylaws.

Report on the Market Analysis for 2010, which was issued by AEC earlier this year, provides the names of all operators and service providers (data controllers) that operated in the country in 2010. Along with the names, the report provides information on the market share of each bigger operator and service provider in a particular electronic communications market. The number of operators and service providers in the specific and most relevant markets is the following:

- Landline phone operators: 35
- Mobile phone operators: 3
- Internet Service Providers (ISP): 75
- Providers of transmission of radio and TV signals to end users: 75

Major player on all these markets is the incumbent operator Makedonski Telekom AD Skopje (T-Home) and its daughter company T-Mobile. This operator has significant market power in the first three above-mentioned markets. Other operators who have significant market share in one or several of these markets are: ONE and its daughter company OnNet (present in all 4 markets), VIP (mobile telephony), CableTel (all markets, except mobile telephony), TeleKabel (all markets, except mobile telephony) and Neotel (landline telephony and ISP).

II. LIST OF ANALYZED LAWS AND REGULATIONS

After reviewing all legal acts that comprise the national legislation in the area of electronic communications, the following pieces were identified as relevant and contain provisions relating to personal data:

- **Law on Electronic Communications** („Official Gazette" no. 13/2005, 14/2007, 55/2007, 98/2008 and 83/2010, Decision of the Constitutional Court U.no.180/2008 published in the „Official Gazette " no.56/2009 and Decision of the Constitutional Court U.no.139/2010 published in the „Official Gazette " no. 171/2010).

- **Rulebook on the Form and Manner of the Single Phone Directory** („Official Gazette " no. 106/2006)

- **Rulebook on Number Portability** („Official Gazette " no. 59/11)

- **Rulebook on the level of information detail to be published in the referent interconnection offers and the manner of their publication** („Official Gazette " no. 154/08 and 40/11)

- **Rulebook on the level of information detail to be published in the offer for unbundled access to local loop and the manner of their publication** („Official Gazette " no. 112/08 and 40/11)

- **Statute of Agency for Electronic Communications** (consolidated version that includes no.13/6 from 19.05.2005, no.11-25/4 from 31.05.2006 and no.11-56/1 from 28.06.2007 and no.11-29/2 from 20.02.2008) (http://www.aek.mk/)

III. ANALYSIS OF PERSONAL DATA RELATED PROVISIONS IN THE ELECTRONIC COMMUNICATIONS LAWS AND REGULATIONS

1. LAW ON ELECTRONIC COMMUNICATIONS

Personal data and the tasks of AEC

Article	Content of the provision	Comment
Article 9, paragraph (1)	For carrying out the activities under Article 8 of this Law, the Agency shall be competent to: "t) Create, maintain and update an electronic database containing information from the electronic communications sector and ensure that the information is available to the public in accordance with the rules on confidentiality and regulations on access to information; ... w) Gather data and information from electronic communications network operators and electronic communications service providers; x) Provide information to the users, operators and service providers, as well	*The task of AEC to make the data from the Register it keeps publicly available (item t) aims to make the operations in this sector more transparent. This data is mainly of business nature (refers to legal entities and their operations). However, in case the electronic database contains personal data, than by interpreting broadly the phrase "in accordance with the rules on confidentiality" personal data protection rules should apply as well.* *The general task of AEC laid down in item w) is regulated in more specific manner further in the law. The way it is written here it might refer and apply to personal data, although the actual aim is to collect data relating to business operations of the providers. If AEC wants to collect specific personal data*

	as to the international organizations and bodies" ...	*from the operators and providers this provision does not provide legal basis for such action.* *Aim of the provision in item x) is to make AEC responsive and cooperative institution, which will share the information it collects and processes with the stakeholders. Again, it primarily refers to the data of business nature.*
Article 21 paragraph (2)	The Agency, the Commission for Protection of Competition and the other state organs and bodies from paragraph (1) of this Article shall exchange data and information they need in exercising their competences, where the scope of exchange of information shall be limited to data and information that is relevant and proportionate to the purpose for which they are exchanged.	*The cooperation and share of information between AEC and the Commission for Protection of Competition will always be related to business-related data. In case the information shared/exchanged with other bodies contains personal data, than this provision enables application of the basic principles of data processing - limited, relevant and proportionate (Article 5 of LPDP)*
Article 23 - Providing Data and Information	(1) Operators of electronic communication networks and electronic communication service providers shall be obliged to make available to the Agency all information, including financial data, which are necessary for the Agency to exercise its competences, including, without any limitation: **...** (2) Requests for information by the Agency shall be justified, based on	*This is a special article that establishes the principles and rules of requesting, sharing and providing data and information between AEC on one side and the operators or other bodies on the other side. The purpose of paragraph (1) is to provide legal power to AEC and oblige other entities to provide information if requested by AEC. It is very unlikely that AEC would*

	reasonable grounds and proportionate to the purpose for which they will be used. (3) Operators and providers of electronic communications networks and/or services shall submit reports, data and information in response to the request of the Agency free of charge and to the extent and within the interval laid down in the request of the Agency. (4) The Agency may only use the confidential information received from another regulatory body for the purposes for which it was requested and shall respect the confidentiality thereof.	*request personal data to exercise its competencies. However, in accordance with paragraph (2) any request of AEC, regardless of the information requested, must follow (personal data protection) principles such as purposefulness, lawfulness and proportionality.* *Paragraph (4) prescribes again that the confidentiality rules shall apply, which clearly suggests that business-related information will be usually requested and received. However, in case personal data is exchanged, than by interpreting broadly the phrase "respect the confidentiality" personal data protection rules should apply as well.*

Article 24 - Records and Storage of Information	(1) The Agency shall keep records and store documentation containing data on: a) operators and service providers; b) users of assigned radio frequencies; c) users of assigned numbers; ...; and h) such other data as the Agency may determine. (2) The Agency shall keep records and store documentation referred to in paragraph 1 of this Article in its information database. (3) The Agency shall keep records and store data on **operators** referring to the following: a) title, principal office, registration court number, unique tax number and name and address of the legal representative for legal entities; b) notification of public communications networks and/or public communications services; c) the date of commencement, alteration or cessation of the provision of public communications services;	*Provisions of this article provide basis for creating and maintaining of several electronic databases by AEC. These provisions clearly set up the type of data that should be stored in these databases and some of that data might relate to physical persons. However, Item h) opens the possibilities of storing various data that is not indicated in this article, simply based on decision of AEC. This could be deemed as contradictory to the LPDP that requires a personal data to be processed only for the purposes specifically written in a law.* *Paragraph (2) prescribes the manner of keeping the records, i.e. for that purpose software applications shall be used. This entails from AEC to introduce and implement technical and organizational measures for providing secrecy and protection of personal data processing at, at least, medium level.* *According to paragraph (3), the database on operators maintained by AEC does not contain any personal data, except for the name and address of the legal representative of the legal entities. The requirement to store the legal representative's personal address might be considered as irrelevant data*

	d) decisions determining operators with significant market power in a relevant market; e) settlement of obligations of operators arising from this Law; f) prescribed penalties for violation of the provisions of this Law.	*and therefore contrary to LPDP.*
	(4) The Agency shall keep the official records and store data on **users of assigned radio frequencies** referring to the following: a) title, principal office, registration court number and unique tax number for legal entities; b) name, address and identification number for natural persons; c) authorizations for the use of radio frequencies; d) settlement of the obligation for the payment of costs for the radio frequency usage; e) prescribed penalties for violation of the provisions of this Law and; f) other records that the Agency may determine.	*According to paragraph (4), AEC maintains official records and stores data on users of assigned radio frequencies, some of which are physical (natural) persons. AEC as Data Controller is obliged to respect the provisions of LPDP. Storing personal identification number has legal ground and it seems necessary in order to identify the natural persons to whom radio frequencies are allocated (contract concluded).*
	(5) The Agency shall keep the following official records and store data on **users of**	*According to paragraph (5), the database on users of assigned numbers*

	assigned numbers: (a) title, principal office, registration court number and unique tax number for legal entities and name and address of a legal representative for legal entities; (b) the decision on assignment of numbers; (c) settlement of the obligation for the payment of costs for the use of numbers; (d) prescribed penalties for violation of the provisions of this Law; (e) other records that the Agency may determine; (6) The Agency may also obtain data listed in this Article from other state bodies and through direct computer or electronic links. (7) The Agency shall retain the data from paragraph 3 of this Article as long as the operator provides public communication service pursuant to this Law, and in the form of an archive for additional five (5) years thereafter. The Agency shall retain the data from paragraphs 4 and 5 of this Article for as long as the natural person or legal entity has the right to use the radio frequency or the number, and in the form of an archive for additional five	*maintained by AEC does not contain any personal data, except for the name and address of the legal representative of the legal entities. The requirement to store the legal representative's personal address might be considered as irrelevant data and therefore contrary to LPDP.* *Provision in paragraph (6) builds upon the provision from Article 21 where it was prescribed that AEC and other state bodies share data. This provision prescribes the manner of obtaining data from other bodies for storage purposes.* *Provision in paragraph (7) relating to the period for which the Agency has a right to keep the data in its records is in compliance with the LPDP, which clearly prescribes that the data should be kept not longer than it is necessary for purposes of processing. Additional 5 years period for data storage is provided in order to be compatible with*

	(5) years after the expiry of such rights.	*the archiving rules.*

Article 25 - Access to Agency Records	(1) The documentation that the Agency keeps in the information database provided for in Article 24 of this Law shall be made publicly available except for confidential records. (2) Subject to section (1) of this Article, the documentation shall contain: a) records of the Agency from Article 24 of this Law, b) records of performed supervision and control, c) data, information, publication of which the Agency believes would contribute to an open and competitive market; d) other records that the Agency may determine. (3) The following records shall not be made publicly available except in cases stipulated in this Law: a) records pertaining to the personnel of the Agency, records of the internal organization and systematisation of the Agency; b) personnel and medical records, and other records the disclosure of which would constitute an invasion of personnel privacy;	*The aim of paragraph (1) is to make AEC records publicly available, with clear exception for the data deemed as "confidential". The meaning and interpretation of confidentiality was previously explained.* *In addition to the records provided in article 24, paragraph (1) sets up what other type of data and documentation AEC could keep and make publicly available, none of which is related to natural persons. Therefore, personal data protection rules do not apply to these additional documents.* *Paragraph (3) clearly makes the exclusion of certain records and data from the obligation to be publicly available, among which is personal data relating to AEC personnel (item a), personnel, medical and other private data (item b) and records that are not publicly available by force of law (item j). This provision eliminates possible ambiguities in the practice relating to public availability of certain records and data, and it is in compliance with LPDP.*

	c) records relating to the defence and security of the country; d) records of information obtained from the services of radio frequency monitoring activities by the Agency; e) records containing information pertaining to the property of operators of electronic communications networks and electronic communications service providers; f) records of trade secrets, commercial financial or technical information of electronic communication networks and electronic communication service providers; g) records submitted to the competent court until the conclusion of the procedure; h) records relating to disputes between operators of electronic communications networks, providers and users of electronic communications services until the conclusion of the procedure; i) records relating to referent offers until their final approval by the Agency's; j) records that are not publicly available by the force of law. (4) The Agency shall make available	*The provision in paragraph (4) relating to the obligation of AEC to provide the*

	records referred to in paragraph (3) of this Article on the request of the courts for court proceedings. (5)The Agency shall be obliged in the forwarding and/or sharing of records with other state bodies containing the information identified in section (3) of this Article to maintain confidentiality applicable to such information. (6) Publicly available records containing information submitted in relation to audits, investigation and examinations shall not be made publicly available until the Agency has acted upon the matter. (7) The Agency in its Statute shall determine the obligations of its personnel pertaining to keeping the confidentiality of records that are not publicly available.	*records and data for the court proceeding purposes is in compliance with LDPD.* *Provision in paragraph (5) relating to sharing of data clearly sets obligation for AEC to respect the confidentiality, which could also be interpreted that if personal data is shared the rules applicable to personal data protection must be followed, especially those relating to technical and organizational measures.* *Provision in paragraph (7) relating to the obligation of AEC to further regulate the obligation of its personnel pertaining to keep the data confidential, is also in line with the provisions of LPDP that require organizational and technical measures to be established by each Data Controller.*

Personal Data and Notification Procedure

Article	Content of the provision	Comment
Article 28 - Notification Procedure	(1) A notification shall be submitted to the Agency prior to the commencement of construction and/or use of public electronic communications networks and/or providing public electronic	*The request to provide the Personal Identification Number and personal address of the legal representative in the statement that the operator encloses to the official notification*

	communications services, alteration or cessation in providing public communications networks and services. (2)The notification from paragraph 1 of this Article must contain, in particular: (a) the name, principal office, the unique tax number and registration number of the entity filing the notification, as well as a statement of the legal representative including his name, address, contact number, and unique identity number;... (3) The notification shall have attached: a) supporting documentation that demonstrates the accuracy and completeness of information from paragraph 1 of this Article, and b) a declaration that the information is accurate and that they meet the conditions provided for in item (b) of paragraph 2 of this Article. (4) Operators and service providers shall be obliged to report the Agency all the changes in the data of paragraph 2 item (a) of this Article provided in the notification, within an interval of thirty (30) days of the occurrence thereof.	*submitted to AEC seems to be obsolete. In addition, paragraph (3) requires supporting documentation to be submitted so that the accuracy of the data provided could be checked, which in a broader sense means that copy of the ID card of the legal representative should be submitted in order to check the accuracy of his/her PIN and address. Taking into account that the statement should not be verified by public notary, the requirement to provide this data and possibly copy of ID card should be deleted. Furthermore, **s**uch requirement is not contained in Article 60 that regulates the authorization request, which speaks for the inconsistency of the Law.* *In order the provision in paragraph (4) to be completely in line with LPDP, than it should also stipulate obligation for AEC to update the notification/database after receiving information on the changes.*

Project implemented by Human Dynamics in association with:
IPS Institute
AlmavivA S.p.A.
Czech Office for Personal Data Protection OPDP
Privacy International

Project office:
Directorate for Personal Data Protection
ul.Samoilova nr.10, 1000 Skopje
Tel: (+389) 2 3230 635

Personal Data and Provision of Overall Phone Directory, Directory Enquiry Service and Public Pay Telephone

Article	Content of the provision	Comment
Article 34 - Provision of Overall Phone Directory, Directory Enquiry Service and Public Pay Telephone	(1) Agency shall prescribe the form and the content of the Overall Phone Directory in which all subscribers in the country are recorded and the same may be published in paper and/or electronic form. (2) The Directory Enquiry Service in the country must provide information from the Overall Phone Directory to all end users, including the users of the public pay telephone. (3) The Agency shall appoint at least one provider of universal service for Overall Phone Directory for the subscribers in the country and it will appoint at least one provider of Directory Enquire Service, under conditions and in a manner determined in Article 33 of this Law. (4) Legal entities and natural persons carrying out business activities shall be obliged to provide data for publishing of, at least, one telephone number in the Overall Phone Directory. (5) Data in the Overall Phone Directory of	*This article was substantially modified in 2010. According to the new provisions of this article, AEC is entitled to prescribe the form and the content of the Overall Phone Directory, unlike the previous provisions that directly prescribed the content of this Directory.* *According to paragraph (4) it is binding for all legal entities and physical persons who carry out business activity to provide, at least, one telephone number to be included in the Overall Phone Directory. This means that this obligation applies only to those physical persons who carry out business activities (e.g. sole traders, free lancers) and to provide only one piece of personal data (phone number), presumably along with the name under which they operate. Therefore, personal data protection rules do not apply to these persons, but also the requirement to provide this data is legal and justified.* *Paragraph (5) sets up the obligation for the providers of both directories to*

	all subscribers in the country should be updated regularly, not less than once a year. Information administered by the Directory Enquiry Service should be updated not less than once a month. (6) Operators providing public pay telephone services shall distribute information about their subscribers to the providers of universal service so that they shall include them without exception in the Overall Phone Directory and in the Directory Enquiry Service. Providers of universal service should immediately notify the Agency if an operator of a public pay telephone service does not provide the requested data, in which case the Agency shall oblige the operator to provide the universal service providers with the requested data within a set time period. (7) If the Agency, based on the opinion of the interested parties, assesses that the public pay telephone service is provided in qualitative manner, it may decide not to introduce it in the whole or part of the territory of the country.	*update the data on annual and monthly basis, respectively. This is in line with the LPDP, which requires the personal data to be accurate and up to date.* *Providers of these three universal services must share data among each other and the provision in paragraph (6) aims to make the exchange of data, including personal data on the subscribers, compulsory for the operators and providers. Such exchange of personal data is legally grounded and justified, because the operators must fulfil obligation set up in law.*

Personal Data and the Register of Assigned Radio Frequencies

Article	Content of the provision	Comment

Article 57 - Register of Assigned Radio Frequencies	(1) The Agency shall keep a Main Frequency Register of existing frequency assignments and their users in the country. (2) The Main Frequency Register shall contain data on the natural persons or legal entities to which specific radio frequencies have been assigned, but shall not include specific radio frequencies used for national security and defence needs and for protection against natural and other disasters. (3) The Agency shall regularly update the Register of assigned radio frequencies. (4) The Agency shall make relevant portions of the Register of assigned frequencies publicly available.	*This article seems to be obsolete, since the Register of assigned radio frequencies is already regulated in Article 24. Although paragraph (2) of this Article prescribes that the register contains data on physical persons, yet most of the users of these frequencies are legal entities or natural persons who perform business activity. Even if personal data is stored, provisions from paragraph (3) and (4) provide for certain principles of personal data protection to be applied.*

Personal Data and the Authorization Issuance Procedure

Article	Content of the provision	Comment
Article 60 - Authorization Issuance Procedure	(1) The Agency shall issue an authorization on the basis of an application for issuance of a radio frequency authorization that must contain the following data: (a) name, address and unique identification number; (b) title, principal office, tax and	*Paragraph (1) of this article prescribes the type of data that the authorization request must contain. In case a physical person requests issuance of authorization for use of radio frequency, then the name, address and personal identification number must be provided, which seems to be quite proportionate to the purpose - physical*

	registration number, bank account number and statement of the legal representative for legal entities; ...	*person will use the frequency for conducting business operations.*

Personal Data and the Numbering Plan

Article	Content of the provision	Comment
Article 77 - Numbering Plan	(4) The Agency shall publish on its website the allocated numbers and series of numbers and the holders of the allocated numbers or series of numbers.	*Holders of the allocated numbers or series of numbers are legal entities, therefore the personal data protection rules do not apply.*

Personal Data and the Subscriber Contract

Article	Content of the provision	Comment
Article 96 - Subscriber Contract	(1) Operators shall provide connection or access to the public communications networks on the basis of contract concluded with subscribers, which must in particular contain the following: (a) name and address of the operator; (b) services provided, the offered service quality, as well as the time for the initial connection; (c) the type and manner of maintenance of services established; (d) detailed information on prices and tariffs, and the time periods for notifying	*Paragraph (1), item (i) provides a right to the subscriber to choose if he/she would like his/her personal data to be included in the Directory Service Enquiry and the Overall Phone Directory, which is in compliance with LPDP (Article 6).*

	any changes thereof; (e) information on the entry into force, duration of the subscriber contract, and the conditions for extension and termination of the subscriber contract, as well as the provision of services; (f) any compensation and the refund arrangements which apply if contracted service quality levels are not met; (g) instructions on how to initiate dispute settlement procedures; (h) obligation to notify subscribers of intended modifications to the conditions in the subscriber contract and instructions on how to accept the new conditions for extension or termination of the contract; (i) possibility for the subscribers data not to be publicly accessible in the Directory Service Enquiry and the Overall Phone Directory (j) procedures in the event of non-payment or untimely payment of services. (2) If the providers of public communications services establish subscriber contracts with end users, such contracts must also contain the elements listed in paragraph 1 of this Article. ...	*This article was amended with paragraph (5) that prescribes the type of data relating to the subscribers, which the operators and providers may keep in their records. The data includes the name, address and personal identification number of the physical persons, which is in compliance with the LPDP (articles 6 and 9). The inclusion of such provision in this article was a good decision by the legislator, because it puts a border line to the personal data that could be processed.* *However, all these provisions prescribe the type of data that must be included in the contracts and records, but leave space for the operators and providers to include other data. Therefore, a provision that will prescribe that collecting and storing personal data other than the data prescribed in paragraphs (1) and (5) shall be prohibited, unless in case of explicit subscriber consent.*

	(5) Operators of the public communication networks and providers of public communication services are obliged to keep records for all subscriber agreements concluded with the users which especially must contain: - name, surname and address, and for the legal entity its title and seat; and - personal identification number or passport number, and for the legal entity its tax identification number.	

Personal Data and Phone Directories and Directory Enquiry Services

Article	Content of the provision	Comment
Article 99 - Directories and Directory Enquiry Services	(1) Subscribers to publicly available telephone services shall have the right to an entry in the overall directory. (2) Operators and providers of public communications services that allocate telephone numbers to subscribers shall be obliged to approve all reasonable requests for the provision of publicly available directory enquiry services and directories, including all relevant data, in a manner and prices available to the public. (3) All end users of publicly available telephone services must have access to the universal directory enquiry services.	*Provisions of this article prescribe the subscriber's rights in relation to Overall Phone Directory and Directory Enquiry Service, including the right to request an entry of data in the directories (paragraph 1), right to access to the directory (paragraph 3) and right to choose the type of personal data that will (not) be publicly available (paragraph 4). All these provisions are in compliance with LPDP where the rights of the data subject are given.* *In addition, paragraph (5) sets up an obligation for the operators to ensure confidentiality of the data (protect the personal data) in the process of*

	(4) The subscriber has the right, upon a previously submitted request to the operator, to choose the data that will not be included in publicly available directory enquiry services or directories. (5) The operators shall be obliged to ensure confidentiality of subscriber data, including its storage, disclosure and usage, in accordance with this and other laws.	*storage, disclosure and usage. Furthermore, this provision makes reference to relevant provisions of this and other laws (primarily LPDP) to be applied.*

Confidentiality and secrecy of the communications

Introductory note. In the following articles the provisions from the Directive 2002/58/EC on Privacy and Electronic Communications have been transposed. The Parliament made an attempt to broaden the scope of application of the provisions in this chapter by adopting amendments to the Law in 2010. These amendments provided broad and unlimited rights to the Ministry of Interior to conduct communication surveillance (without court's order), while at the same time obliged the operators and providers of public communication networks to make adjustments and provide technical possibilities for such surveillance. But most importantly, these provisions would have seriously violated the human rights, especially the right of privacy. Most of these provisions were objected by group of non-governmental organizations, who jointly submitted application to the Constitutional Court. After reviewing the amendments and the application, the Constitutional Court decided to annul these provisions on the basis of their incompliance with Article 8 of the Constitution. Few provisions remained in force, but they are practically inapplicable without the annulled provisions. Eventually, the current provisions in this chapter are those from the original text of the Law and are largely in compliance with the EU Directive on Privacy and Electronic Communication.

Article	Content of the provision	Comment
Article 110 - Protective	(1) Operators of public communications networks and service providers of communications services shall be	*Provisions of this article set up an obligation for the operators and providers to adopt appropriate*

Measures	obliged individually, and jointly where necessary, to adopt appropriate technical and organizational measures to ensure the security of their networks and/or services. (2) Such measures must ensure a level of security and protection appropriate to the reasonable foreseeable risks, the determination of which may take the technical feasibility of the measure into account. (3) Operators of public communications networks and service providers of public communications services shall be obliged to inform their users of particular network security risks and the means whereby users can reduce such risk, as well as of the potential costs covered by the users, if the risk lies outside the scope of measures which the operator may take.	*technical and organizational measures to ensure the security of the networks and services. This is entirely in line with the provisions of LPDP, Rulebook on Organizational and Technical measures for providing secrecy and protection of personal data processing and eventually the EU Directive on Privacy and Electronic Communication.* *However, this article fails to include the amendments to the EU Directive on Privacy and Electronic Communication that specify the minimum measures that must be taken by the operators and providers to safeguard the security and provide power to the national authority to audit the measures taken (Article 4 item 1a).* *Also, it does not include the amendments that require the user and the national authority to be informed in case of personal data breach and the measures that should be undertaken thereupon (Article 4 items 3 and 4).*
Article 111 - Confidentiality of Communications	(1) Confidentiality of communications shall apply to: a) the content of communications;	*Paragraph (1) prescribes the type of data to which the principle of confidentiality shall apply. It applies to the content, traffic data, locations*

	b) traffic data and location data relating to communications; and c) unsuccessful attempts to establish a connection.	*data and even to the unsuccessful attempts to establish a connection.*
	(2) All forms of surveillance, interruption, recording, storage, transfer and diverting of communications and data referred to in paragraph (1) of this Article are hereby prohibited, except in cases where it is necessary for the purpose of conveyance of a message as a fax message, electronic mail, electronic mailbox, voice mail, SMS message, and others or being in compliance with the provisions of Article 112, 114, 115-a and 115-b of this Law.	*Paragraph (2) clearly specifies the types of actions (forms) that are illegal and prohibited. But it also provides the exceptions to this general rule. Both - prohibition and exceptions - are line with the EU Directive on Privacy and Electronic Communications.*
	(3) Operators and providers of public communications networks and services, their agents, employees, representatives, and other parties under their direction and control, shall protect the confidentiality of communications, which obligation shall survive the cessation of the activities in which they were obliged to protect such confidentiality.	*Paragraph (3) contains provision similar to the confidentially clauses in the business contracts, thus enabling ceaseless protection of confidential data.*
	(4) Operators and providers of public communications networks and services, their agents, employees, representatives, and other parties under	*The remaining paragraphs of this article provide more precise rules referring to the exceptions, i.e. when*

	their direction and control, may obtain, use or provide confidential communications information to others only to the extent essential for the provision of specific public communications services. (5) If operators and providers of public communications networks and services need to obtain information on the content of communications, or copy or store communications and related traffic data, they shall be obliged on entering subscriber contracts or at the start of provision of public communications services to inform the user, and to erase the information on the content of communications or the communications, as soon as technically feasible, after the information or communication is no longer required for the provision of the specific public communications service. (6) Subscribers or users may record communications, but they shall be obliged to inform the sender or recipient of the communication thereof or adjust the operation of the recording device so that the sender or recipient of the communication is informed of its operation. (7) Recording of communications and	*the operators and providers are entitled to process confidential and personal data. They are all in line with the EU Directive on Privacy and Electronic Communications (Article 5).*

	the associated traffic data shall be permitted with the objective of securing evidence of market transactions or any other business communications, or within organizations receiving emergency calls, for their registration, identification and resolution. (8) The use of electronic communications networks to store data or gain access to data stored in the terminal equipment of subscribers or users for further processing shall only be permitted in cases where the operator of public communications networks and the provider of public communications services: a) informs in advance the subscriber or user of the purpose of processing of such data; b) gives the subscriber or user the right and opportunity to refuse such processing; and c) provides the subscriber or user with a designated point of contact to which to communicate such refusal. (9) Storage of or access to data shall be permitted for the sole purpose of faster carrying out the transmission of a message over an electronic communications network, or if essential	

	for the provision of an information society service which the subscriber or user explicitly requested.	
Article 112 - Traffic Communication Data	(1) Operators and providers of public communications networks and services are obliged to keep unprocessed the traffic data for the last 24 months. (2) Operators and providers of public communications networks and services may store and process traffic data required for billing and interconnection payments until payment for services. (3) Providers of public communications services may, for the purpose of marketing electronic communications services or for the provision of value added services, process traffic data only on the basis of the subscriber's or user's prior consent. Subscribers or users must be informed of the types of traffic data processed and the duration of such processing prior to giving consent. Users or subscribers shall have the right to withdraw their consent at any time. (4) Operators and service providers of public communications networks shall be obliged to stipulate in the subscriber contract the manner of storage, duration and processing of traffic data and to declare that they shall handle	*Provisions of this article are in compliance with the EU Directive on Privacy and Electronic Communications (Article 6), except for paragraph (1). The provision in this paragraph was added in 2010 and replaced the previous one that was in line with the wording in the Directive. Namely, if the traffic data should be kept for 24 months, by analogy, the traffic data must be erased after the expiration of that period, as it is required by the Directive. But, this should be made clear in order the provision to be completely in line with the Directive. Also, 24 months period for* keeping the traffic data unprocessed *seems to be too long and not in line with the current trends of decreasing the period of storage of such data.*

	them in accordance with this Law. (5) Traffic data may only be processed by the responsible persons with the operator of public communications networks or service provider of public communications who are responsible for billing or traffic management, customer enquiry response, fraud detection, electronic communications services marketing, or provision of value added services, and the processing must be restricted to the extent that is necessary for conducting the activities. (6) Operators and service providers of public communications networks shall be obliged to keep the traffic data from paragraph (1) of this article in the country. (9) Operators and service providers of public communications networks shall be obliged to provide the traffic data upon written request by the Agency for the purposes of conduct of dispute resolution and other proceedings pursuant to this Law.	
Article 113 - Calling and Connected Line Identification	(1) The operator or service provider of public communications networks who offers calling line identification, shall be obliged to enable the calling user, before each call, to use the possibility, using simple means and free of charge,	*The provisions of this article are in compliance with the EU Directive on Privacy and Electronic Communications (Articles 8 and 10)*

	of preventing the presentation of the calling line identification. The provider of public communications services shall be obliged to provide its subscribers, to automatically and free of charge prevent the identification for all calls from their lines. (2) Operators and service providers of public communications networks shall be obliged to override the prevention of calling line identification for emergency calls. (3) The operator or service provider of public communications networks who offers calling line identification, shall be obliged to enable the called user, before each call, to use the possibility, using simple means and free of charge, of preventing the presentation of the calling line identification. (4) If an operator or service provider of public communications networks offers called line identification and the identification is possible prior to the line being established, the called subscriber must have the possibility, using simple means, of rejecting incoming calls where the calling line identification has been prevented by the called user or subscriber. (5) If an operator or service provider of	

	public communications networks offers called line identification, it shall be obliged to enable the called user, to use the possibility, using simple means and free of charge, of preventing the connected line identification to the calling user. (6) If a subscriber requests in writing that the operator trace malicious or nuisance calls, the operator or service provider of public communications network may temporarily record the origin of all calls ending in the network termination point of such subscriber, including those for which prevention of calling line identification has been requested. (7) Data on tracing must be stored and supplied to the subscriber who requested tracing of malicious or nuisance calls and the same are also delivered to the competent body pursuant to the conditions and in the manner stipulated in Article 115 of this Law. (8) Operators and service providers of public communications networks shall be obliged in their general conditions for conclusion of subscriber contracts to determine the possibility of presentation and prevention of calling	

	and connected line identification. (9) Provisions of this Article shall apply to subscriber lines connected to digital exchanges and to analogue exchanges only if such requirements are technically feasible or would not cause disproportionate costs.	
Article 114 - Location Data	(1) Location data other than traffic data relating to users or subscribers may be processed only in anonymous form or on the basis of a prior consent by the user or subscriber to the extent and for the duration necessary for the provision of a value added service. (2) Users or subscribers may withdraw such consent at any time. (3) Users or subscribers, prior to giving their consent for data processing, must be informed about the following: a) the type of data to be processed, b) the purpose and duration of such processing, and c) the possibility that location data may be transmitted to third parties for the purpose of providing the value added service. (4) Users or subscribers who have consented to the processing of location	*The provisions of this article are in compliance with the EU Directive on Privacy and Electronic Communications (Article 9). The provision in paragraph 6 (obligation to supply the location data referring to emergency call numbers to the competent body responding to emergency calls), which adds one more possibility for processing of location data, is not taken from the Directive. Since such possibility is already present in the Directive for the calling line identification presentation, this provisions should be deemed as compliant with the rules of the Directive.*

	data from paragraph 1 of this Article shall have the possibility, using simple means and free of charge, of temporarily refusing the processing of such data for each connection to the network or for each transmission of a communication. Processing of location data without the data shall be permitted to persons employed with the operator or service provider of public communications services or to third parties providing value added services. (5) Location data from paragraph 1 of this Article may only be processed by competent persons with the operator or provider of public communication services or by third parties providing value added service, and the processing must be restricted to the extent that is necessary for the provision of the value added service. (6) Operators shall be obliged to supply the location data referring to emergency call numbers to the competent body responding to emergency calls, in appropriate technical manner.	
Article 115-a – Measures and activities that enable	(1) Operators and service providers of public communications networks shall be obliged to provide surveillance of the communications in real time to the	*After the Constitutional Court has annulled the article 115 on the basis of unconstitutionality, these two articles (115-a and 115—b) became*

communication surveillance **Article 115-b – Storing and protection of the data from the communication surveillance**	competent body for communication surveillance. Information on the surveillance communication should be available upon end of the communication, while the surveillance of the communication should be uninterrupted at all times during the communication. (2) Operators and service providers of public communications networks shall be obliged to provide accurate and unified linkage of the information on the communication that is under surveillance with the content of the communication that is under surveillance. (3) In case operators and service providers of public communications networks have introduced cryptographic protection, they are obliged to remove such protection, i.e. to use decryption system before the content of the communication service has been submitted to the competent body for communication surveillance. (4) Operators and service providers of public communications networks should secure that the persons whose communication is under surveillance or other unauthorized persons do not notice any change in the quality of the	*meaningless and inapplicable. Provisions of these two articles prescribe the manner and techniques of conducting specific actions relating to the surveillance, but they cannot be taken without the basis for conducting surveillance that was given in the annulled article.* *Law on Communication Surveillance is the right place to put these provisions, since they refer to the communication for the purpose of public security and defence, which is excluded from the application of electronic communications legal framework.*

	communication that is under surveillance which might be caused by the application of communication surveillance measure. The functioning of the communication that is under surveillance should not be modified for the person whose communication is under surveillance. (5) Operators and service providers of public communications networks should secure same or bigger level of security and quality of the communication that is under surveillance compared with the security and quality of the communication services provided to the person whose communication is under surveillance. **115-b** Operators and service providers of public communications networks shall be obliged to keep the data on the equipment, interface and all other data relating to the application of communication surveillance measure as classified information and to secure their protection in accordance to the law.	
Article 116 - Automatic Call Forwarding	(1) Subscribers must have the possibility, using simple means and free of charge, of stopping automatic call forwarding by a third party to their	*The provision of service of automatic call forwarding (paragraph 1) will be offered under the condition that is technically feasible and not costly*

	terminal equipment. (2) The provision from paragraph 1 of this Article shall apply only if the implementation is technically feasible or would not cause disproportionate costs.	*(paragraph 2). EU Directive on Privacy and Electronic Communications (Article 11) does not specify that provision of this service will be conditional, but indirectly such condition may be applied. Namely, article14 of the Directive specifies that if certain service can be offered only by implementing specific technical features in electronic communications networks, than Member States shall inform the Commission.*
Article 117 - Unsolicited Communications	(1) The use of automated calling systems for making calls to the subscribers' telephone numbers without human intervention (eg. facsimile machines or electronic mail), for the purposes of direct marketing, may only be allowed if subscribers have given their prior consent. (2) Natural or legal entities having electronic mail addresses from the customers of their products or services may use such addresses for direct marketing of their similar products or services, but they shall be obliged to give their customers the possibility at any time, free of charge and using simple means, of preventing such use of their electronic address. (3) The sending of electronic mail for	*The provisions of this article are in compliance with the EU Directive on Privacy and Electronic Communications (Article 13), except for paragraph (3) which fails to include "electronic mails that encourage recipients to visit websites" in addition to "electronic mail for the purposes of direct marketing". But, there is no need to amend this provision, because this missing part might be considered as included by broadly interpreting the term "direct marketing".*

	the purposes of direct marketing disguising or concealing the identity of the sender on whose behalf the message is sent, or without a valid address to which the recipient may send a request that such communications cease, shall be prohibited.	
Article 118 - Subscriber Data	(1) Operators may obtain the following data on their subscribers: a) name or title of the subscriber; b) identity number for natural persons, and tax and registration numbers for legal entities; c) activity of the subscriber, at his request; d) address of the subscriber; e) subscriber's number; f) at the request of the subscriber, academic title before, and occupational title after the name of the subscriber; g) on the basis of payment, additional data if so desired by the subscriber, provided that this does not encroach on the rights of third parties; and h) regularity of payment. (2) Data stated in paragraph 1 of this	*Provisions in this article are not based on the Directive. However, they are in compliance with the LPDP and basic personal data processing rules. Namely, type of data that operators may collect is necessary for conducting their activities and providing their services.* *In addition, paragraph (2) clearly specifies the limited purposes for which the collected and stored data may be used, thus preventing the possibilities for (ab)use of personal data for other purposes.* *Eventually, paragraph (3) limits the period of storage of this data by setting up precise time period (1 year), which is objective and necessary for the purposes of other laws (e.g. taking legal action against subscriber who has not paid a bill is possible within a year from the due date).*

	Article may only be used for: a) concluding, monitoring and termination of subscriber contracts; b) billing for services; and c) the preparation and issuing of subscriber directories in accordance with this Law. (3) On termination of a subscription, data from paragraph 1 of this Article must be stored for one (1) more year from the date of issuance to the subscriber of the latest bill for services provided, and if during such interval an order is issued by the competent body for the storage and transmission of such data, for the period stipulated by the order of the competent body.	
Article 119 - Directories	(1) Subscribers must be informed free of charge of the purposes of directories and of the use of such data before being included in printed or electronic directories available to the public. The costs of informing subscribers shall be borne by the publisher of the directory. (2) Subscribers must have the opportunity to determine which, if any, of their personal data from paragraph 1 of Article 118 will be included in a public directory. Subscribers may verify their	*The provisions of this article are in compliance with the EU Directive on Privacy and Electronic Communications (Article 12).*

	personal data or require their correction or erasure. (3) Refusal to be included in a public directory, and verifying, altering or erasing personal data shall be free of charge.	

Misdemeanours and penalties relating to personal data breach in the electronic communications

Article	Content of the provision	Comment
Offences	(1) A fine in the amount of 7 to 10% of the total annual revenue acquired during the commercial year prior the year when the misdemeanour was performed or of the total revenue acquired for a shorter period of the year preceding the misdemeanour, provided that the legal entity commenced its operations during that year shall be imposed to the legal entity if it: … 26) undertakes surveillance, tapping, interruption, recording, storage and diverting of communications and data in instances forbidden by this Law (Article 111, paragraph 2); 27) keep unprocessed the traffic data for the last 24 months or do not keep them in the country (Article 112, paragraphs 1 and 6)	*Three of these misdemeanours and penalties prescribed for the perpetrators (items 30, 31, and 32) relate to the breach of provisions that are either annulled by the Constitutional Court or have become meaningless because the provisions they refer to are inapplicable (articles 115-a and 115-b).* *The other two penalties (items 26 and 27) can be imposed for misdemeanours relating to personal data breach, which is in line with and required by the EU Directive (Article 15-a).*

	30) fails to ensure at its own expense adequate equipment and appropriate interfaces for lawful tapping of communications (Article 115, paragraph 1 and 3); 31) fails to commence the measures and activities that enable communication surveillance (Article 115-a); 32) fails to ensure storage and protection the data from the communications surveillance (Article 115-b); ...	
Article 139	(1) A fine in the amount of 4 to 7% of the total annual revenue acquired during the commercial year prior the year of performing the misdemeanour or of the total revenue acquired for a shorter period of the year preceding the misdemeanour, provided that the legal entity commenced its operations during that year shall be imposed to the legal entity if it: … 18) fails to protect confidentiality of data, exchanged when concluding a contract for interconnection or access (Article 44, paragraph 3); … 39) fails to adopt technical and organizational measures for the security of its network and/or services (Article 110, paragraphs 1 and 2);	*Misdemeanours and penalties prescribed in this article are less severe than the previous one, but still severe enough to achieve the goal. These penalties relate to the breaches of the provisions from the articles regulating the secrecy and confidentially of the communication, where, to repeat, provisions of the EU Directive are transposed. Almost all actions taken by the operators or other persons that violate the privacy of the subscribers and users are subject to penalties. Same conclusion given in the note on the previous article can be made for these penalties – they are in line with and required by the EU Directive (Article 15-a).*

	40) fails to warn its subscribers of the specific risks for the security of the network (Article 110, paragraph 3); 41) fails to protect the confidentiality of electronic communications (Article 111, paragraph 3); 42) acquires for itself or for another party information on the contents, facts and circumstances of transmitted messages in excess of the minimum necessary extent essential for the provision of specific electronic services, or fails to use such information solely for the provision of such services and compliance with contractual undertaking relating thereto (Article 111, paragraph 5); 43) fails to inform the users in a clear and understandable manner about the control and purpose of processing of data, or fails to offer an opportunity for refuting such data processing, or fails to obtain the consent of a user prior to the processing of data (Article 111, paragraph 8); 44) processes traffic data without the prior consent of the user or subscriber (Article 112, paragraph 3); 45) allows traffic data to be processed by persons that are not authorized to do	

	that (Article 112, paragraph 5); 46) fails to process location data in accordance with Article 114 paragraph 1 of this Law; 47) limits the right of the user or subscriber to temporary rejection of location data processing (Article 114, paragraph 4); 48) allows that location data be processed by persons that are not authorized to do that (Article 114, paragraph 5); 50) uses electronic communications for direct marketing without the consent of the subscriber (Article 117, paragraph 1); 51) uses the electronic address of customers for direct marketing without allowing the customers to refuse such direct marketing (Article 117, paragraph 2); 52) uses a false identity or false address in direct marketing with the use of electronic communications (Article 117, paragraph 3);	
Article 140	(1) A fine in the amount of 2 to 4% of the total annual revenue acquired during the commercial year prior the year of performing the misdemeanour	*According to the national legislator misdemeanours and penalties prescribed in this article are less severe than the ones prescribed in the*

	or of the total revenue acquired for a shorter period of the year preceding the misdemeanour, provided that the legal entity commenced its operations during that year shall be imposed to the legal entity if it: … 15) fails to ensure calling line and called number identification and prevention thereof (Article 113 paragraph 1); 16) in the general conditions for concluding a subscriber contract fails to stipulate the possibility of calling line and called number identification and prevention thereof (Article 113, paragraph 8); 17) fails to inform the users or the subscribers of the elements of Article 114, paragraph 3 of this Law before they provide consent for processing the data; 18) fails to offer subscribers or users the possibility of temporarily refusing the processing of location data (Article 114, paragraph 4); 19) uses subscriber data collected in contravention to Article 118, paragraph 2 of this Law; 20) fails to inform subscribers free of charge of the purpose of subscriber	*previous two articles. Indeed, these penalties can be imposed to the breach of privacy which will not have negative consequences as those in the previous articles. Same conclusion given in the note on the previous two articles can be made for these penalties – they are in line with and required by the EU Directive (Article 15-a).*

	directory and the usage of the data prior to including them in a printed or electronic directory (Article 119, paragraph 1); 21) fails to provide subscribers with the opportunity to determine whether and which of their personal data will be included in the public directory (Article 119, paragraph 2); 22) refusal to be included in a public subscriber directory and the verification, alteration or erasure of personal data claiming that such services are not free of charge (Article 119, paragraph 3);...	

2. RULEBOOK ON THE FORM AND MANNER OF THE SINGLE PHONE DIRECTORY

This short Rulebook (3 pages and 6 articles) simply collects in one place all provisions from the Law on Electronic Communication that relate to the Single (Overall) Phone Directory. It was adopted in 2006 and never amended, though it should be, at least, because of the replacement of the word "Single" with "Overall" in the amendments to Law on Electronic Communications. For the purpose of this analysis, the following provisions of this Rulebook are taken into account:

Article 2 – Purpose of the Rulebook

"The purpose of this Rulebook is to provide availability of the data from the Directory to all subscribers in the country, as part of the provision of universal service."

The concept of universal service promoted by the Universal Service Directive 2002/22/EC, which is incorporated and further regulated in the Law on Electronic Communications, means availability of the package of basic services (provision of services to all end users regardless of their geographical location) and affordability of these services. In that direction, all subscribers (end users) in the country should have access to the Overall Phone Directory. It means that the operator who provides this universal service (Single Phone Directory) should make the Directory available, i.e. provide access to all subscribers in the country regardless of the operator(s) with whom the subscribers have contract. All data contained in the Directory must be available; but the type of data that will be contained in the Directory is regulated in the other articles of this Rulebook.

Article 4 - Single (Overall) Phone Directory

"(3) Single (Overall) Phone Directory should contain data especially for:

- *subscribers who are natural persons: name, surname, possibly titular, address and phone number*
- *subscribers who are legal and physical entities: name and address of the entity and all its branches and phone numbers*

This provision contains two unclear words, which makes it difficult to assess compliance of the provisions with the personal data processing rules and principles. First, the word "titular" could have several meanings, especially taken into account the place it is put, i.e. it could refer to: a) title of the person (Mr. or Mrs. or Ms.), b) professional title of the person (e.g. lawyer), educational title of the person (e.g. MA, PhD) or honourable title (e.g. His Excellency) and c) person's ownership, which is most unlikely. Whatever is meant, this data reveals information about a person, i.e. data that identifies or could identify one or more characteristics of the person. Second, the phrase "physical entities" used in the second item of this paragraph, which is also used throughout the entire text of the Law on Electronic Communications, refers to those natural persons who perform business activities. As of that reason, these physical entities are legally treated as legal entities in terms of data that should be provided.

Nevertheless, the type of data that the Directory should contain based on these provisions is not excessive. Processing of this data, i.e. making this data available to a wider public (all subscribers) has its legal basis in the Law on Electronic Communications.

Article 6 – Obligations to provide data for the Single (Overall) Phone Directory

"(3) Operators of public communication networks (landline and mobile) do not provide data in the Single (Overall) Phone Directory for those subscribers who had requested in writing the data not to be published in the Directory."

Provision with similar wording and basically same meaning is already contained in the Law on Electronic Communications. Both provisions provide right to the subscriber his/her personal data not to be included in the Overall Phone Directory, under a condition his/her request to be made in writing (in order to have evidence). This provision is in compliance with LPDP and the "opt-out" principle.

3. RULEBOOK ON NUMBER PORTABILITY

This Rulebook regulates the manner, time period, technical conditions for implementation of portability of portable numbers, and rules for implementation, operation and maintenance of Central Referent Database of Number Portability (CRDNP). The aim of this Rulebook is to boost competition on the market by providing a right to the subscriber to keep the same number when changing the network end point within the same geographical numerical area and/or the operator/provider of public communication network or service.

The Rulebook mainly contains technical rules that should be followed by the operators when the subscriber requests number portability service. However, in the course of this process personal data is transferred from one to another operator and as of that reason there are several provisions regulating this aspect. Another set of provisions regulate CRDNP (database maintained by AEC or entity authorized by AEC) where different types of data, including personal data, is stored. These are the most relevant provisions from the aspect of personal data processing, but it must be noted that almost all the other provisions have indirect relevance since they introduce technical measures for providing security of the electronic database and communication.

Article 3 - Definitions

*"(j) **Central Referent Database of Number Portability** is created with the aim to enable number portability and contains information on routing related to all portable numbers. The legal entity that administers this database provides information to all operators and other users who have such right based on law or bylaw.*

...

*(l) **Local Database of Transferred Numbers** is a database located at the operator, contains data necessary for routing of the call to the transferred number and it is used in real time upon establishing a call to the transferred number."*

Article 4 – Responsibilities of operators

"(7) Operators and operators-users will share the entire information related to number portability procedure, through CRDNP, while in a written form the recipient operator will submit one sample of the original request for concluding subscriber contract for number portability to the provider operator not later than 5 days from the day the request was received.

(9) Operators and operators-users should upon reception of the request for number portability check the identity of the subscriber and check the following data:

- *Verification of the identity (name, surname and Personal Identification Number)..."*

(10) The recipient operator is responsible for the submitted request for number portability, the data contained therein as well as for the verification of the identity ... If the submitted request for number portability is based on false identity of the subscriber, which is noticed by the provider operator... than the recipient operator shall cover all the damages to the provider operator and the subscriber."

Law on Electronic Communications provides basis for exchange of data between the operators. Provisions in article 4 precise the type and manner of exchange of data for the purpose of number portability. It is not disproportionate request subscriber's basic personal data to be exchanged, including his/her Personal Identification Number, as a way to verify the real identity of the person. If the identity of the subscriber is not determined correctly, then the recipient operator could suffer severe consequences (payment of damages).

Article 7 – Initiating number portability

"(2) Request for concluding subscriber contract for number portability shall include:

...

- *(item 7) explicit consent of the subscriber that the recipient operator may transfer the data contained in the request to the provider-operator and to AEC..."*

According to this provision there must be an explicit written consent given by the subscriber prior to any data transfer. This is in line with Article 6 of LPDP that requires previously given consent by the Data Subject (in this case the subscriber) for processing of his/her personal data.

Article 13 – Developing, managing and maintaining the CRDPN system

"AEC will develop, manage and maintain CRDNP through an internal organizational unit or by delegating these tasks to another natural or legal person, which will be selected through a public call."

This provision provides possibility for AEC to transfer the task of developing, managing and maintaining the database, which may happen due to limited and inadequate capacities and resources of AEC. Personal data protection rules require that the involved parties in such case must conclude contract, which will include obligation for the entity, to which the responsibility for administering the database (data processing) is transferred, to implement personal data protection measures. Yet, it would be good solution if such provision/obligation is added in this article as well.

Article 14 – Content of CRDNP and manner of their processing

Provisions in this article structured in eight paragraphs regulate the manner of data processing, i.e. provide technical rules for the involved parties. These provisions provide for implementation of high security standards such as secure and protected link for exchange of data and access to the database, system of logs to which only system administrators have access, etc. The last paragraph prescribes that AEC will publish on its web site detailed technical description of the transactions and the communication interface between CRDNP and operators.

Article 15 – Data Management

Provisions of this article structured in seven paragraphs built upon the previous one and prescribe the time period for communication and transactions between CRDNP and operators. Furthermore, there are provisions that determine responsibilities of AEC and operators relating to update and accuracy of the data exchanged.

These two articles prescribe the technical measures that should be applied in order to provide security of the data processed. There is a space for additional measures to be added in this Rulebook

or at least a provision that will state that AEC will adopt additional internal document where the entire set of technical and organizational measures for providing secrecy and protection of personal data processing will be prescribed. Since this Rulebook is adopted by AEC Director (meaning that authority to adopt internal acts of general application cannot be delegated), it seems that this Rulebook is the appropriate legal act to introduce such technical and organizational measures.

Article 18 – Entry and check of entry of the transferred number

"(2) The entry for the transferred number should contain:

...

(f) name, surname and Personal Identification Number..."

Only the data specified in item (f) is of personal nature. All other data relates to the technical parameters necessary for the number to be transferred. In addition to the name and surname a PIN is requested to be entered, because it is a unique identifier of the persons, which is crucial from a technical point of view. There is also legal base in the Law on Electronic Communication for AEC to collect this data and for the operators to exchange it. Therefore, this provision/requirement is in line with the personal data protection rules.

Article 20 – Termination of use of transferred number

"(3) CRDNP will delete the information relating to the number of serial of numbers in the database upon receipt of notification that the number is no longer in use."

This means that the data, including personal data, will be deleted because is no longer necessary to be processed. This is in compliance with LPDP (Article 5).

Annex 2 – Template for request for concluding subscriber's contract for number portability

This template contains one more data that must be filled in by the subscriber – his/her father name. This personal data should not be requested because it is: a) not indicated in Article 7 where the content of the request is prescribed and b) too excessive for the purpose (name, surname and PIN is sufficient to identify the person).

4. RULEBOOK ON ESTABLISHING THE LEVEL OF INFORMATION DETAIL TO BE PUBLISHED IN THE REFERENT INTERCONNECTION OFFERS AND THE MANNER OF THEIR PUBLICATION

This Rulebook prescribes the level of the information detail contained in the referent interconnection offer and the manner of their publication by operator with significant market power in the market for public landline voice telephone networks and services or operator with significant market power in the relevant market for public mobile telephone networks and voice services (hereinafter referred to as: Operator), the contents of the reference offer, obligation for submission and approval of the reference offer to AEC, the realization of interconnection, including the manner and procedure for concluding interconnection agreements. Actually, this Rulebook aims to set up clear business relations between the Operator and all other operators for interconnection purposes by prescribing the type of information, mainly of business and technical nature, which must be provided and published. Therefore, it has limited effect over personal data.

Article 2 - Definitions

*"**(j) Calling Line Identity Data** (CLI) is the number of the user who is making the call which is transferred through the operators' networks per each call;*

***(k) Calling Line Identification Presentation** (CLIP) is a service for presentation of identification data of the calling line;*

***(l) Calling Line Identification Restriction** (CLIR) is a service that prevents presentation of identification data of the calling line."*

Article 9

"(3) When the data for identification of the calling line are transmitted to the Operator's network, the Operator transmits the data to the called end user if service CLIP has been used.

(4) When the data for identification of the calling line are transmitted to the Operator's network, the Operator does not transmit the data to the called end user if service CLIR has been used, except when it comes to the call to emergency services calls."

The provisions cited above refer to the calling line identification data, which is considered as private and personal data due to the possibility for the end users to identify the person who is making the call. Basic rules relating to calling and connected line identification are given in Article 113 of the Law on Electronic Communications, while these provisions repeat the rules using bit more technical wording. These rules clearly stipulate what needs to be done by the Operator if the subscriber requested or gave its consent for use of these services.

5. RULEBOOK ON ESTABLISHING THE LEVEL OF INFORMATION DETAIL TO BE PUBLISHED IN THE REFERENT OFFERS FOR UNBUNDLED ACCESS TO LOCAL LOOP AND THE MANNER OF THEIR PUBLICATION

This Rulebook prescribes the level of the information detail to be published in the referent offer for unbundled access to local loop and the manner of their publication by the operator with significant market power on the relevant markets for public landline voice telephony networks and services (hereinafter: Operator), content of the referent offer, realisation of the unbundled access to the local loop, as well as the manner and procedure for concluding the general agreement for unbundled access to the local loop, the procedure for the referent offer approval by AEC and submitting of report. Like the previously elaborated Rulebook, this one also aims to set up clear rules of the game between the Operator and all other operators who want to use the unbundled access to local loop. The data published and processed is mainly of business nature, except for the data contained in the articles cited below.

Article 10 – Obligations for unbundled access to local loop

"(4) The Operator shall offer to the User-operator access to its support systems, information systems, as well as to its databases for preparation of orders, deliveries, maintenance, repair requests and invoicing. In order to grant an access, the Operator should provide technical specifications for the interface of its information system in the referent offer."

This provision sets up an obligation for the Operator to provide access to its databases, where among other data, subscribers personal data is stored. It is assumed that the technical specification will prescribe appropriate technical and organizational measures that will secure protection of the personal data. It is not necessary to stipulate all possible measures in this Rulebook, but provision that will oblige the Operator to prescribe and implement such measures might be added.

Article 13 – Realization of unbundled access to local loop

"(1) The Operator starts to provide unbundled access to specific local loop or sub-loop if the Operator has written request by the subscriber to whom the electronic communication service should be provided.

(2) The request from paragraph (1) of this Article should contain, at least, identification data of the subscriber and its signature, as well as the type of service that should be provided by the user-operator.

(3) ...User-operator may request from the Operator, with whom the subscriber has concluded subscriber contract, information whether the subscriber has regularly fulfilled its obligations from the subscribers contract and the provided information may be used as basis for the User-operator to reject the request of the subscriber."

The requirement from paragraph (2) to fill-in identification data in the subscriber's request is rational. However, it should be specified the type of personal data that should be provided. The way is now laid down, leaves space for the operators to request various and numerous types of personal data, relevant and proportionate to the purpose. The possibility given in paragraph (3) might affect the subscriber's privacy, but it is proportionate to the risk that user-operator takes by concluding the subscriber's contract and providing its services.

6. STATUTE OF THE AGENCY FOR ELECTRONIC COMMUNICATIONS

This Statute regulates the scope and responsibilities of AEC, the bodies of AEC, representation, internal organization, recruitment and deployment of employees, rights and responsibilities of the employees, the manner of work of AEC, employees' obligations in terms of keeping the confidentiality of data, and other issues of importance to the functioning of AEC.

In terms of competencies and tasks of AEC, this Statute repeats the competencies and tasks already given by the Law on Electronic Communications, including the ones of relevance for the personal data processing.

Article 25

"(7) The Commission shall prescribe the manner of access to data and information that the Agency is obliged to publish and to other data and information."

This provision delegates a power to the highest body of the Agency, the Commission, to prescribe detail rules relating to the manner of access to the publicly available data, but also to other type of data. Taking into account that personal data is deemed as confidential in accordance with Article 28 of the Statute, than the rules adopted by the Commission, at least those referring to the public data, will not apply to the personal data processing.

Article 28 – Confidentiality of data

"As confidential data shall be deemed the data contained in the acts, documents, information and publications that are not publicly available in accordance with the law.

The following acts and documents are deemed as confidential:

1) acts for persons employed in the Agency and acts on the internal organization and systematization of the Agency;

2) personal and health documentation for staff and other documents whose disclosure would mean a violation of privacy;

...

10) documents not available to the public by force of law.

Acts and documents referred to in paragraph 2 of this article must be marked as confidential.

The President and members of the Commission, Director and employees in the Administrative Office of the Agency shall not use information or documents or content thereof, which are considered as part of official documentation of the Agency or obtained through or in connection with their engagement or employment, except as part of the performance of their duties. They may not publish information marked as confidential in accordance with the law, bylaws, Statute and other general acts of the Agency, whether in reduced scale, in written or oral form, directly or indirectly to any person outside the Agency. Information or documents available to the public in regular operations are not subject to this prohibition.

The prohibition in this paragraph applies to decisions adopted by the Commission on sessions before they are released to the public.

The President and members of the Commission, the Director of the Agency and employees in the Administrative Office of the Agency, as well as other legal and natural persons to which the Agency entrusted the execution of certain tasks are required to keep the confidentiality of the data that is not publicly available, regardless of how they have obtained the data."

Provision in paragraph (1) on the type of data that is deemed as confidential repeats the text from the provision with similar wording contained in the Law on Electronic Communications. It is clearly specified in item 2) that the personal data shall be treated as confidential. The subsequent provisions of this article specify the bodies and persons to whom confidentiality obligation refer to and what the confidentiality actually means (prohibited actions).

Project implemented by Human Dynamics in association with:
IPS Institute
AlmavivA S.p.A.
Czech Office for Personal Data Protection OPDP
Privacy International

Project office:
Directorate for Personal Data Protection
ul.Samoilova nr.10, 1000 Skopje
Tel: (+389) 2 3230 635

SUMMARY AND RECOMMENDATIONS

- In general, there is a high level of compliance of the entire national legal framework on electronic communications with the personal data processing rules and principles. This refers to the Law on Electronic Communications and the bylaws adopted on the basis on this law. Main reasons for achieving the compliance are the following: a) Law on Electronic Communications was drafted and enacted practically in the same time with the drafting and enactment of the Law on Personal Data Protection and b) the Law incorporates the provisions from the EU Directive on Privacy and Electronic Communications.

- Very small number of amendments to the Law and/or bylaws is necessary to be adopted in order to: a) achieve complete compliance of the national electronic communication legislation with the EU and national legislation and best practices in the area of personal data protection and b) bolster the protection of the right to privacy and personal data of the subscribers and users of electronic communication networks and services.

- Throughout the entire text of the Law on Electronic Communications and some of the bylaws, the words “confidential data” and “confidentiality” are used. In some cases when determining the type of data that is deemed as confidential the personal data is explicitly included. The phrase “in accordance with the rules on confidentiality” might and should be interpreted broadly so that the personal data protection rules could apply as well. However, it would be even better if the following could be added in the Law and bylaws “in accordance with the rules on confidentiality and protection of personal data” or if the Law defines the scope and meaning of the term “confidential data”. In that way, it won’t be necessary to rely on broad interpretations and personal data protection rules will apply directly.

- Taking into account that this Law, to a large extent, regulates business relations among the operators/providers or relations between AEC and operators/providers, it is understandable why emphasis is given on “confidential data” and “confidentiality”. Most of the data collected, shared and stored among AEC and operators is of business and technical nature, although sometimes this is not specifically indicated and might be read that personal data is processed as well. In some cases, personal data is subject of processing, especially in the provisions referring to subscribers and users. In those cases, personal data protection rules apply.

- Article 24 of the Law that regulates the records and storage of information gives right to the Agency to determine other types of data that it may collect and store. This opens possibilities of storing various data that is not indicated in this article, simply based on decision of AEC. This could be considered as contradictory to the LPDP that requires a personal data to be processed only for the purposes specifically written in a law. It might be added that "other type of data" does not refer to personal data.

- According to article 24 paragraphs (3) and (5) the database on operators and database on users of assigned numbers, both maintained by AEC, do not contain any personal data, except for the name and address of the legal representative of the legal entity. The requirement to store the legal representative's personal address might be considered as irrelevant data and therefore contrary to LPDP.

- Same refers to Article 28 paragraph (1), which requires Personal Identification Number and personal address of the legal representative to be written in the statement that the operator encloses to the official notification submitted to AEC. In addition, paragraph (3) of this article requires supporting documentation to be submitted so that the accuracy of the data provided could be checked. This would mean that copy of the ID card of the legal representative should be submitted in order to check the accuracy of his/her PIN and address. Taking into account that the statement should not be verified by public notary, the requirement to provide this data and possibly copy of ID card should be deleted. In order the provision in paragraph (4) of this Article to be completely in line with LPDP, than it should also stipulate obligation for AEC to update the notification/database after receiving information on the changes.

- Article 96 prescribes the type of data that must be included in the subscribers' contracts and records, but the way it is written also leaves space for the operators and providers to include other data. Therefore, a provision that will prescribe that collecting and storing personal data other than the data prescribed in paragraphs (1) and (5) shall be prohibited, unless in case of explicit subscriber consent.

- Article 110 prescribes the protective measures that must be implemented, but it fails to include the amendments to the EU Directive on Privacy and Electronic Communication that: a) specify the minimum measures that must be taken by the operators and providers to safeguard the security, b) provide power to the national authority to audit the measures taken and c) require the user and the national authority to be informed in case of personal data breach and the

measures that should be undertaken thereupon. For that purpose, amendments to the Law are necessary.

- The provision in Article 112 paragraph (1) is not quite in compliance with the EU Directive on Privacy and Electronic Communications. Namely, it clearly requires traffic data to be kept unprocessed for 24 months, but it does not prescribe that it must be erased after the expiration of that period, as it is laid down in the Directive. This should be made clear in order the provision to be completely in line with the Directive. Also, 24 months period for keeping the traffic data unprocessed seems to be too long and not in line with the current trends of decreasing the period of storage of such data.

- After the Constitutional Court has annulled the article 115 on the basis of unconstitutionality, articles 115-a and 115-b (measures and activities that enable communication surveillance and manner of storing and protection of the data from the communication surveillance) became inapplicable. Provisions of these two articles prescribe the manner and techniques of conducting specific actions relating to the surveillance, but they cannot be undertaken without the basis for conducting surveillance that was given in the annulled article. In addition, Law on Communication Surveillance is the right place to put these provisions, since they refer to the communications for the purpose of public security and defence, which is excluded from the application of electronic communications legal framework.

- According to article 116 paragraph (1), provision of automatic call forwarding service will be offered under the condition that is technically feasible and not costly. EU Directive on Privacy and Electronic Communications (Article 11) does not specify that provision of this service will be conditional, but indirectly such condition may be applied. Namely, article 14 of the Directive specifies that if certain service can be offered only by implementing specific technical features in electronic communications networks, than Member States shall inform the Commission.

- Provision in Article 117 paragraph (3) fails to include “electronic mails that encourage recipients to visit websites” in addition to “electronic mail for the purposes of direct marketing”, as laid down in EU Directive on Privacy and Electronic Communications . But, there is no need to amend this provision, because this missing part might be considered as already covered by broadly interpreting the term “direct marketing”.

- Only one provision in the Rulebook on Single (Overall) Phone Directory could be amended due to the two unclear words it contains ("titular" and "physical entities"), which might have affect on personal data processing. If these words are clarified, then it would be easier to assess whether the request to collect them is relevant and proportionate to the purpose.

- Articles 14 and 15 from the Rulebook on Number Portability prescribe the technical measures that should be applied in order to provide security of the data processed. There is a need for additional measures to be added in this Rulebook or at least a provision that will state that AEC as owner of the system will adopt additional internal document where the entire set of technical and organizational measures for providing secrecy and protection of personal data processing will be prescribed.

- Annex 2 of the Rulebook on Number Portability is actually a template for request for concluding subscriber's contract for number portability. This template contains one more data that must be filled in by the subscriber – his/her father name, which should not be requested because it is: a) not indicated in Article 7 where the content of the request is prescribed and b) too excessive for the purpose (name, surname and PIN is sufficient to identify the person).

- Article 10 from the Rulebook on the level of information detail to be published in the referent offers for unbundled access to local loop and the manner of their publication sets up an obligation for the Operator to provide access to its databases, where among other data, subscribers personal data is stored. It is assumed that the technical specification will prescribe appropriate technical and organizational measures that will secure protection of the personal data. It is not necessary to stipulate all possible measures in this Rulebook, but provision that will oblige the Operator to prescribe and implement such measures might be added.

- Article 13 paragraph (2) of the same Rulebook requires subscriber's identification data to be filled-in in the subscriber's request. It should be more precise and specify the type of personal data that needs to be provided. The way is now formulated, leaves space for the operators to request various and numerous types of personal data, which might not be relevant and proportionate to the purpose.