1.

The positive legal framework of the Republic of Serbia, governing this field, for the most part complies with international standards and the EU acquis.

In this field, capacities at the normative and institutional level have increased in the past few years with the definition of privacy protection objectives, development of an appropriate system, promotion of cooperation and creation of responsibilities of all stakeholders at the national level, which also includes protection of privacy in the context of digital communication.

The Republic of Serbia ensures respect for and protection of the right to privacy by applying the following legislation:

- **The Personal Data Protection Act** ("Official Gazette of the RS", No. 97/2008). The aim of this Act is to ensure realization and protection of the right to privacy and other rights and freedoms regarding personal data processing to every natural person. Personal data protection tasks are performed by the Commissioner for Information of Public Importance and Personal Data Protection as an autonomous state body, independent in the execution of his or her competences. The Act has awarded the following rights: the right to information on personal data processing, the right to insight, the right to copy, the right of data subject regarding insight performed and restrictions of rights, a request for realization of a right, and decision-making. The Act specifically defines competence, data provision, records, transfer of data from the Republic of Serbia, monitoring and penalty provisions.

- **The Electronic Communications Act** ("Official Gazette of the RS", Nos. 44/2010 and 60/2013 – the decision of the Constitutional Court):

• Article 3 defines objectives and principles of regulating relations within the electronic communications sector which are base on: 12) ensuring a high level of protection of personal data and user privacy, in accordance with the Personal Data Protection Act and other acts;

• Article 37 defines activities in the electronic communications sector which shall be carried out under the regime of general authorization and/or in accordance with general conditions that may be prescribed for all or certain types of electronic communications networks and services according to the provisions of this Act. General conditions refer to the conditions concerning the following: 14) protection of personal data and privacy within the electronic communications sector, in accordance with provisions of this Act and acts regulating protection of personal data;

• Article 41 defines that the operator shall supply all necessary data and information of relevance for the performance of activities which fall within the scope of the Republic Agency for Electronic Communications, at the request of the Agency, in particular the data and information pertaining to: 8) ensuring protection of personal data and privacy of users, and assessing security and integrity of electronic communications networks and services, including implementation of policies on security, continuity of work and data protection;

- **The Telecommunications Act** ("Official Gazette of the RS", Nos. 44/2003 and 36/2006):

• Chapter 8 Supervision, Article 24 defines authorization for exercising supervision. Supervision of conducting activities in the telecommunications sector and the use of the radio frequency spectrum is exercised by the Republic Agency for Electronic

Communications. In exercising the supervision referred to in paragraph 1 of this Article, the Agency is authorized to: 5) examine compliance of public telecommunications operators with the obligations stipulated herein pertaining to tariffs, universal service, interconnection, leased lines, privacy and security of information, as well as with other obligations stated herein, and to take measures to remedy the irregularities established with the operators;

- LICESES FOR PUBLIC TELECOMMUNICATIONS NETWORKS AND PUBLIC TELECOMMUNICATIONS SERVICES are issued in accordance with the principles for granting operating licenses where any natural person or legal entity may construct, own or operate a public telecommunications network and/or provide public telecommunications service if the Agency has previously granted them the relevant license, unless otherwise stipulated under this Act. Article 39 stipulates that the license shall also contain information and conditions related to: 15) rules for the protection of personal data and privacy specific to a particular field of telecommunications;
- Obligations of public telecommunications operators – privacy and security of information are described in Article 54. The public telecommunications operator shall take all the relevant technical and organizational measures so as to ensure confidentiality and security of its services and shall not be permitted to disclose information about contents, terms and conditions of message transmission beyond the minimum level necessary for providing services on the market or in cases stipulated under the law. The public telecommunications operator may keep and process the tariff data which refer to individual customers and which are processed for the purposes of establishing connections, only to the extent necessary for customer billing purposes. The public telecommunications operator may provide the data referred to in paragraph 2 of this Article only to the sender and recipient of messages at their request.
- Article 55 prohibits any activity or use of equipment threatening or interfering with the privacy and confidentiality of messages transmitted via telecommunications networks, except in the case consent has been obtained from customers or in case theses activities are performed in compliance with the law or a court order issued in accordance with the law.

2.

At the normative level, ranging from the Constitution of the Republic of Serbia, a systemic act in this area – the Personal Data Protection Act – to the provisions contained in other acts – the Electronic Communications Act, the Classified Information Act, the Criminal Code, the Criminal Procedure Code – ensure protection of privacy which is, for the most part, at the level of protection in developed democratic and organized societies.

At the institutional level, establishment of new state authorities and bodies and improvement of work and capacities of existing state authorities and bodies, particularly independent state and regulatory authorities and supervisory bodies, ensured improvement of the national system which is capable, with the application of the positive legislation, to ensure respect for the right to privacy of the citizens of the Republic of Serbia, *inter alia*, by timely recognition and adequate response to the occurrence of unlawful and illegal threats to this right.

Taken measures are described in the following legislation:
- **The Electronic Communications Act** ("Official Gazette of the RS", Nos. 44/2010 and 60/2013 – the decision of the Constitutional Court):

• Chapter XVI Security and integrity of public communications networks and services, Article 125 defines that the operator shall inform the Republic Agency for Electronic Communications of any violations of security and integrity of public communications networks and services that significantly affected their operation, and particularly of violations that caused infringement of personal data protection or privacy of subscribers or users.

• Special competences of inspectors are defined in Article 134. Apart from the competences resulting from the act governing execution of inspection activities, an inspector shall be authorized to verify: 6) actions of operators related to the implementation of measures of personal data and privacy protection, provision of security and integrity of public communications networks and services, and enabling lawful interception of electronic communications and access to retained data.

- **The Organization and Competences of Government Authorities Combating Cyber Crime Act** ("Official Gazette of the RS", Nos. 61/2005 and 104/2009). This Act regulates the formation, organization, competences and authorizations of special organizational units of government authorities for the purposes of detection, prosecution and trials for criminal offences specified in this Act. This Act shall apply for the purposes of detection, criminal prosecution and trials for: 3) criminal offences against freedoms and rights of a man and a citizen.

3.

In terms of relevant legislation governing this area: the Constitution, the Criminal Procedure Code (CPC), the Electronic Communications Act (ECA), the Security-Intelligence Agency Act, the Military Security Agency and Military Intelligence Agency Act and other acts establish the highest known standards for interception of communications, either by the insight into contents of communications, or without any insight into contents (access to telecommunications traffic), stipulating existence of a previous decision of a judicial body as a condition for interception.

The Constitution in Article 41 guarantees that the confidentiality of letters and other means of communication is inviolable. Derogation shall be allowed only for a specified period of time and based on a decision of the court if necessary to conduct criminal proceedings or protect the safety of the Republic of Serbia, in a manner stipulated by the law.
Interception of electronic communications that reveals the contents of communications in the Republic of Serbia shall not be permitted without the prior consent of the user, except for a definite time and based on a court decision, if necessary for criminal proceedings or protection of security of the Republic of Serbia, in a manner prescribed by the act (Article 126(1) of ECA).

As for the manner prescribed by the law, lawful interception of electronic communications may be conducted on the basis of CPC, the Security-Intelligence Agency Act and the Military Security Agency and Military Intelligence Agency Act.

The field of retained data in the Republic of Serbia is regulated by the Electronic Communications Act (hereinafter referred to as ECA) whose provisions are largely in line with Directive 2006/24/EC of the European Parliament and of the Council.

ECA prescribes a general obligation of public telecommunications operators (hereinafter referred to as the operator) to keep the retained telecommunications traffic data for the period of 12 months after the communication has taken place (Article 128(4) of ECA).

The same Article of the Act in paragraph 1 defines that the operator shall retain data on electronic communications for the purposes of conducting an investigation, detecting criminal offences and conducting criminal proceedings, as well as for the purposes of protecting national and public security of the Republic of Serbia.

The stated retained data are listed in Article 129(1) of ECA, and the Article in paragraph 3 explicitly prescribes that data revealing the contents of a communication may not be retained.

Retained data in the Republic of Serbia shall be, according to the positive legislation regulating this field, deemed personal data.

Existing regulations in the Republic of Serbia certainly aim to provide a high level of protection of personal data and privacy of users and to ensure security and integrity of public telecommunications networks and services. *The Strategy for Development of Electronic Communications in the Republic of Serbia for the period 2010-2020* ("Official Gazette of the RS", No. 68/10) emphasized commitment to the regulations of the European regulatory framework:

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;
2) Directive 2002/20/EC of the European Parliament and of the Council of 7 March 2002 on the authorization of electronic communications networks and services - Authorization Directive;
3) Directive 2002/19EC 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;
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 - Authorization Directive;
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;
6) 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 Communication (BEREC) and the Office;
7) 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 service, 2002/19/EC on access to, and interconnection of electronic communications networks and associated facilities, and 2002/20/EC on the authorization of electronic communications networks and services;
8) 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;
9) 2000/417/EC: Commission Recommendation of 25 May 2000 on unbundled access to the local loop: enabling the competitive provision of a full range of electronic communications services including broadband multimedia and high-speed Internet (notified under document number C(2000) 1529) (Text with EEA relevance);
10) Stability Pact Electronic South Eastern Europe Initiative and Electronic South Eastern Europe Initiative (eSEE) Agenda+, 27 February 2004;
11) Final Acts of the Regional Radiocommunication Conference for planning of the digital terrestrial broadcasting service in parts of Regions 1 and 3, in the frequency bands 174-230 MHz and 470-862 MHz (RRC-06);
12) Communication from the Commission to the Council, the European Parliament, the European Economic and Social Committee and the Committee of the Regions and accelerating the transition from analogue to digital broadcasting (COM(2005) 204);
13) Commission Decision of 6 May 2010 on harmonized technical conditions of use in the 790-862 MHz frequency band for terrestrial systems capable of providing electronic communications services in the European Union (notified under document C(2010) 2923) (Text with EEA relevance) (2010/267/EU);
14) European Convention for the Protection of the Audiovisual Heritage (ETS no. 183);
15) Recommendation Rec(2003)9 of the Committee of Ministers to member states on measures to promote the democratic and social contribution of digital broadcasting.

4.

The Constitution of the Republic of Serbia in Article 42(2) prohibits the use of personal data for any purpose other than the one they were collected for, and it shall be punishable in accordance with the law, unless this is necessary to conduct criminal proceedings or protect safety of the Republic of Serbia, in a manner stipulated by the law.

Personal data, including personal data collected by intercepting communications, practically have multiple normative protection through the existence of a systemic act in this field – the Personal Data Protection Act, the Classified Information Act and ECA, which prescribe taking measures of security and protection against accidental or unauthorized destruction, accidental loss or alteration, unauthorized or unlawful storage, processing, access or disclosure, to limit access to retained data in an appropriate manner only to authorized persons, so that they could be used only for the purpose for which they were collected, and to limit their use and storage, after what time they will be deleted from databases and registers.

Positive legal norms in the Republic of Serbia ensure control and supervision of collection of personal data by intercepting communications by the Court (previously – by deciding on the application, later – by reporting on results of application to the court that adopted a decision), by executive authorities (by controlling work of administrative authorities, by issuing binding directives and orders, by reporting), as well as by legislation authorities (either directly or through parent committees, by passing an act or by supervising the work of state authorities).

Article 146 of the Criminal Code prescribes fines and penalties for unauthorized collection, processing and use of personal data.

The legal system of the Republic of Serbia guarantees an individual's right to an effective remedy and the right to be informed when it comes to the collection of personal data in this way:
– In addition to the quoted paragraph 3 of Article 42 of the Constitution, paragraph 4 of the same Article guarantees that everyone shall have the right to be informed about personal data about him or her, in accordance with the law, and the right to court protection in case of their abuse;
– The judge for preliminary proceedings may inform the person against whom a secret supervision of communication was conducted, if during the conduct of the action his or her identity was established and if it would not threaten the possibility of conducting criminal proceedings (Article 163(2) of CPC);
– The Personal Data Protection Act (Article 23) determined the right of citizens to information, the right of insight and the right to copy of the data collected about them;
– Due to conducted inspection, the data subject has the right to request correction, amendment, updating or erasure of data as well as termination and temporary recess of processing if the purpose and manner of processing are not clearly determined or unauthorized, or if the data being collected are disproportionate to the purpose or are incorrect (Article 22);
– In addition to the above stated, any person who believes that individual activities or actions of a state authority violate or deny his or her rights and freedoms, may, for the purposes of protecting his or her rights, refer to the Ombudsman, competent committee of the National Assembly of the Republic of Serbia, the Government and other competent authorities and institutions of the Republic of Serbia, as well as to the bodies of internal control of the police and to the security service.

The Sector for Electronic Communications, Information Society and Postal Services of the Ministry of Foreign and Internal Trade and Telecommunications manages a special working group for the preparation of the wording of the Information Security Bill.

The Republic of Serbia adopted the national standard SROS ISO/IEC 27001:2011 (Information Technologies – Security Techniques – Information Security Management Systems – Requirements) – Connection with the international standard ISO/IEC 27001:2005 ISO/IEC JTC 1/SC 27.
Adoption of the standard related to the latest version of ISO/IEC 27001:2013 is expected to take place.

5.

The right to the protection of personal data is regulated by the Personal Data Protection Act, as part of the right to privacy. This Act does not distinguish between the right to protection in terms of an information carrier, therefore it refers both to the protection of data in a digital form as well as in the, so called, non-digital world. The basis for data processing may be a legal norm or person's consent. The Act, however, conditions that person's consent must be given in writing, which also implies an electronic form, under conditions stipulated in the Act regulating electronic signatures, which results in the fact that this Act is not technologically neutral.

The Commissioner for Information of Public Importance and Personal Data Protection (hereinafter referred to as the Commissioner) is an independent and autonomous body established by the Free Access to Public Information Act ("Official Gazette of the RS",

Nos. 120/04, 54/07, 104/09 and 36/10), whose competence was extended by the Personal Data Protection Act ("Official Gazette of the RS", Nos. 97/08 and 104/09 – another act, 68/12 – the decision of the Constitutional Court, and 107/12). Competences of the Commissioner are regulated by Article 35(1) of the Free Access to Information of Public Importance Act and Article 44(1) of the Personal Data Protection Act. In the field of data protection, the Commissioner shall, *inter alia*, supervise implementation and execution of the Act and/or monitor implementation of data protection, decide on appeals in cases stipulated by this Act, maintain the Central Register, monitor and allow transfer of data from the Republic of Serbia, provide an opinion about the formation of new data collections and/or, in case of introduction of new information technologies, about data processing, also monitors arrangement of data protection in other countries, and cooperates with the authorities competent for the supervision of data protection in other countries. A report on Commissioner's work for 2013, which also contains a report on the implementation of the Personal Data Protection Act, is submitted to the National Assembly of the Republic of Serbia and is available on the Commissioner's website (http://www.poverenik.rs/sr/o.nama/godišnji-izveštaji/1772-izveštaj-poverenika-za - za 2013-godinu.html).

In terms of monitoring, more precisely, the interception of communications between persons and access to retained data on electronic communications, we would refer to the Electronic Communications Act. In particular, we would point out the Decisions of the Constitutional Court adopted for the purposes of the Proposal for the assessment of the constitutionality of the Military Security Agency and Military Intelligence Agency Act ("Official Gazette of the RS", No. 88/09) and the Electronic Communications Act ("Official Gazette of the RS", No. 44/10) which was jointly filed by the Ombudsman and the Commissioner. In terms of the Military Security Agency and Military Intelligence Agency Act, we refer to the Decision IUz-1218/2010 of 19 April 2012, published in the "Official Gazette of the RS", No. 55/2012 of 1 June 2012, and in terms of the Electronic Communications Act, which refers to the access to retained data, we refer to Decisions Us IUz No. 1245/2010 of 13 June 2013, published in the "Official Gazette of the RS", No. 60/2013 of 10 July 2013. We also refer to the Proposal of the Commissioner and the Ombudsman for the assessment of the constitutionality of the Criminal Procedure Code submitted to the Constitutional Court on 19 May 2012.

The Commissioner initiated the process of supervision of the implementation and execution of the Personal Data Protection Act in terms of the operators who provide "broadband access" services and/or access to the Internet by natural persons. Information about the process is available on the Commissioner's website (htt://www.poverenik.rs/sr/saopštenja/1764-zabrinjavajuci-rezultati-nadzora-nad.operatorima-interneta.html).