Balancing the interests in the context of data retention (INVODAS)

Bulgaria

Raina Nikolova

Part 1: General overview of the legal transposition, the national (societal) context and the constitutional/fundamental rights legal framework

A. State of play of the transposition of the Directive 2006/24/EC

I. Legal provisions

- *Introductory remark:* If national legal provisions mandating the retention of electronic communications data without any *specific* reason (i.e. stockpiling, without an actual, concrete cause) have existed already before the Directive 2006/24/EC (in the following: "the Directive") was enacted, please also make reference to these when answering to questions 5 to 35.

- *Introductory remark:* Most of the questions concerning retention obligations refer to the national provisions transposing the Directive. Some questions, however, make explicit reference to the "national law" or the "national legal system" as a whole. In these cases, we request you to provide more comprehensive information. In any case, only retention *without a specific reason* (i.e. stockpiling, without an actual, concrete cause) of data generated or processed in *electronic communications* is concerned by this questionnaire. Other retention obligations, for instance those requiring that there be a suspicion of a crime having been committed, are not covered by this questionnaire.

1. Have the provisions of the Directive already been transposed into national law?

The provisions of the Directive are currently transposed in full in the Electronic Communications Act, promulgated in State Gazette, issue 41 dated 22 May 2007, as subsequently amended and supplemented (the "ECA"), and in Ordinance No 40 on Data Types and Terms and Conditions for Retention and Dissemination of Data by Providers of Electronic Communications Networks and/or Services for the Purposes of the National Security and Criminal Investigations, promulgated in State Gazette

issue 9 dated 29 January 2008, as subsequently amended and supplemented (the "Ordinance").

- ***If transposition has <u>not at all</u>, or only in <u>parts</u>, been accomplished:***

2. **What are the reasons for the transposition not (or only in parts) to have been effected (e.g. (purely) formal delays in the legislative procedure, constitutional law concerns, legal policy issues, socio-ethical concerns, incompatibility with the national legal system etc)?**

   Not applicable.

3. **Is transposition still intended? If so: What is the current state of play of the transposition process? Until when is it likely to be finalised?**

   Not applicable

4. **In case draft legal acts are existent, or a law that had already been enacted/come into force has subsequently been abrogated by a court decision or for other reasons: Please describe the content of the provisions on the basis of questions 5, and 7 to 35.**

   Not applicable.

- ***If transposition has been <u>accomplished</u>:***

General questions

5. **Is there an English version of the texts available? If so: Please indicate the respective URL.**

   There is no an up-to-date English version of the texts of the ECA and the Ordinance. The Bulgarian texts of the ECA and the Ordinance No 40 are available on the Internet:

   ECA: http://lex.bg/bg/laws/ldoc/2135553187

   Ordinance No 40: http://www.lex.bg/bg/laws/ldoc/2135577924

6. **Since when have the relevant regulations been in force? Are there any transition periods in place regarding the application of these regulations?**

   The ECA came into force on 25 May 2007. The Ordinance regulating in details the terms and conditions for data retention was adopted on 7 January 2008 and came into effect on 1 February 2008 (the provisions of the Ordinance concerning the Internet access and Internet networks entered into force on 15 March 2009). Non-governmental organizations appealed the Ordinance before the Supreme Administrative Court claiming that some of its provisions (and especially Art. 5 of the Ordinance) allow the Ministry of Interior to control the activities of the mobile operators and are directly violating the right to privacy protected by the Bulgarian

Constitution and the European Convention on Human Rights and Freedoms. The procedural argument of the applicants was that the Ordinance is a secondary piece of legislation and therefore cannot contravene to higher ranked legislation – the Constitution and the ECHR. The Supreme Administrative Court repealed Art. 5 of the Ordinance effective from 19 December 2008. As a result, the Ministry of Interior of the then ruling coalition government proposed most of the provisions of the Ordinance to be enacted in the ECA. The Parliament approved the proposed bill and the amendments to the ECA came into force in March 2009.

In the summer of 2009 parliamentary elections were held and a new government by the right-wing Political Party GERB was formed. The new government proposed to the Parliament new substantive changes to the ECA, which came into force on 10 May 2010. By way of this amendment, the most important matters of the Data Retention Directive were implemented on a primary legislative level, and thus ceased to be part of the Ordinance, which is considered as a secondary legislative act.

7. **What type of legal act do the existing rules meant to transpose the Directive's provisions pertain to (e.g. Act of Parliament, decree-law, regulation/decree, administrative provisions etc)? Please give an overview of all legal provisions enacted for this purpose (stating the type of legal act and the matter regulated therein) and describe**

   a) **whether "more important" matters have been dealt with by (parliamentary-enacted) legislation whereas provisions of a more technical/technology-oriented character are tackled by decrees/administrative provisions, and**

   b) **whether the types of legal acts chosen for the different matters regulated correspond to those usually chosen in your legal system for such kind of matters.**

Currently, the Directive's provisions are implemented in an act of the Parliament, i.e. the Electronic Communications Act. However, some definitions and rules concerning the data retention are still regulated by the Ordinance, which is a secondary legislative act adopted by the Minister of Interior.

The ECA regulates the following areas related to data retention: (i) Obligation for data retention; (ii) Categories of data to be retained; (iii) Period of retention; (iv) Competent authorities that can gain access to retained data; (v) The procedure to be followed in order to gain access; (vi) Supervisory authorities and their powers for monitoring the application of the data retention rules; (vii) material definitions, and (viii) penalties for violation of the data retention rules.

The Ordinance governs in further details (i) the categories of the data to be retained, (ii) the statistical requirements, and (iii) other definitions.

As explained above, some matters regarding data retention are still regulated by both, the ECA and the Ordinance. Consequently, there are certain overlaps between

the two acts in terms of their scope of regulation, i.e. categories of data to be retained, definition, etc. Although the overlaps do not lead to any material discrepancies between both acts it is recommendable that the provision of the Ordinance, which repeat the relevant texts of the ECA be repealed in the future. Thus, both acts will be put in compliance with the below requirements of the Law on Normative Acts.

According to the Law on Normative Acts provides a legislative act (e.g. ECA) shall govern on a primary level constant public relations, while secondary legislation (e.g. Ordinance) shall be adopted in order to provide more detailed regulation of the matters already covered by a legislative act.

8. **Are the terms defined in art. 2 para. 2 of the Directive also defined within the national law transposing the Directive? If so: To what extent do the definitions given therein differ from those in art. 2 para. 2? Are there any other terms mentioned in the Directive or in the directives referred to by the Directive (see the reference made in art. 2 para. 1 of the Directive to Directives 95/46/EC, 2002/21/EC and 2002/58/EC) that have also been legally defined in national legislation?**

All terms defined in Art. 2, para 2 of the Directive are also defined in Para 1 of the Additional Provisions of the ECA and Para 1 of the Additional Provisions of the Ordinance. The definitions contained in the ECA and the Ordinance do not deviate from the terms mentioned in the Directive or the other relevant directives.

The definition of "user" is contained in item 49 of Para 1 of the Additional provision of the ECA: "User means any legal entity or natural person using or applying to use a publicly available electronic communications services". The definition of a "subscriber" is laid down in item 1, para 49 of the Additional Provisions of the ECA: "Subscriber means any natural or legal person, party to a contract with an undertaking providing public electronic communications services". Analysing the definitions of use and subscriber in the ECA altogether, it can be concluded that although the definition of the term "user" is the ECA is shorter than the one contained in the Directive, it complies with the legal concept implied in the term "user" in the Directive.

Given below is a full list of the other relevant definitions:

All other definitions of the Directive are contained in Para 1 of the Ordinance. These definitions are absolutely identical to the ones given in Directive, namely:

"Data" means traffic data and location data and the related data necessary to identify the subscriber or user (item 1).

"Fixed and mobile telephone service" means calls (including voice, voicemail and conference and data calls), supplementary services (including call forwarding and call transfer) and messaging and multi-media services (including short message services, enhanced media services and multi-media services (item 2).

"User ID" means a unique identifier allocated to persons when they subscribe to or register with an Internet access service or Internet communications service (item 3).

"Cell ID" means the identity of the cell from which a mobile telephony call originated or in which it terminated (item 4).

"Unsuccessful call attempt" means a communication where a telephone call has been successfully connected but not answered or there has been a network management intervention (item 5).

Dimension 1 (State - citizen)

9. What data have to be retained according to the national rules transposing the Directive? Do these rules include additional retention obligations with regard to traffic data that go beyond the obligations mentioned in the Directive (e.g. location data resulting from the use of mobile email services), or do national retention obligations fall short of those specified by the Directive? Do data on unsuccessful call attempts have to be retained?

The categories of data to be retained are laid down in the ECA, namely data necessary to (i) trace and identify the source of the communication; (ii) identify the destination of the communication; (iii) identify the date, time and duration of the communication; (iv) identify the type of the communication; (v) identify the communications terminal equipment of the user or what purports to be a communications terminal equipment of the user; (vi) identify the location label (cell ID)[1].

The data necessary to trace and identify the source of the communication should refer to (i) the calling telephone number and data necessary to identify the subscriber or user (in the case of a public telephone service), or (ii) the user ID as allocated, the user ID and telephone number as allocated to any communication entering the public telephone network, the data necessary to identify the subscriber or user to whom an Internet Protocol (IP) address, user ID or telephone number was allocated at the time of the communication (in the case of Internet access, Internet electronic mail and Internet telephony)[2].

The data required to identify the destination of the communication should refer to (i) the telephone number dialled (the telephone number called) and, in cases involving supplementary services such as call forwarding or call transfer, the number or number to which the call is routed and data necessary to identify the subscriber or user (in the case of a public telephone service), or (ii) the user ID or telephone number of the intended recipient(s) of an Internet telephony call, data necessary to identify the intended recipient of the communication (in the case of Internet electronic mail and Internet telephony)[3].

---

1 Art. 250a, para 1.

2 Art. 251a, para 1.

3 Art. 251a, para 2.

The data necessary to identify the date, time and duration of the communication should refer to (i) the date and time of the start and end of the communication (in the case of public telephone service), or (ii) the date and time of the log-in and log-off of the Internet access service, based on a certain time zone, together with the IP address, whether dynamic or static, allocated by the Internet access service provider to a communication, and the user ID of the subscriber or register, the date and time of the log-in and log-off of the Internet electronic mail service or Internet telephony service, based on a certain time zone (in the case of Internet access; Internet electronic mail and Internet telephony)[4].

The data required to identify the type of the communication should refer to (i) the type of the public telephone service used, or (ii) the Internet service used (in the case of Internet electronic mail or Internet telephony)[5].

The data requested to assist in identifying the communications terminal equipment of the user should refer to (i) the calling and the called telephone numbers (in the case of fixed telephone service), (ii) the calling and called telephone number, the International Mobile Subscriber Identity (IMSI) of the calling party, the International Mobile Subscriber Identity (IMSI) of the called party, the International Mobile Equipment Identity (IMEI) of the mobile electronic communications terminal equipment of the calling party, the International Mobile Equipment Identity (IMEI) of the mobile electronic communications terminal equipment of the called party; in the case of pre-paid services: the date and time of the initial activation of the service and the location label (Cell ID) from which the service was activated, and data necessary to identify the subscriber or user (in the case of public telephone service provided through a terrestrial mobile network), or (iii) the calling telephone number of dial-up access, the digital subscriber line (DSL) or other end point of the originator of the communication (in the case of Internet access, Internet electronic mail and Internet telephony)[6].

The date necessary to identify the location label includes the administrative addresses of a terrestrial mobile electronic communications network in which a call originated or terminated (Art.251a, Para 6).

The Ordinance also contains an obligation for data retention in case of unsuccessful call attempts (Art.2, Para 2).

---

4 Art. 251a, para 3.

5 Art. 251a, para 4.

6 Art. 251a, para 5.

10. Does national law otherwise provide for, or allow for, the retention of electronic communications data (customer records, traffic data and/or the content of communications) beyond the data to be retained in accordance with the Directive? Please specify the substance of these provisions.

The ECA provides for some additional possibilities for retention of electronic communications data by providers of electronic communications networks and/or services, which fall outside the scope of the Directive.

Firstly, they are authorised to collect, process and retain traffic data, which is necessary for provision of electronic communications services, for billing, for the preparation of the subscriber bills, as well as for proving their reliability.

Secondly, the providers are allowed to retain location data, which indicates the geographic position of the electronic communications terminal equipment of the user.

The above-mentioned data may be used by the undertakings providing public electronic communications services for the following purposes:

1. Detecting, locating and eliminating defects and software errors in the electronic communications networks.

2. Detecting and terminating unauthorized use of electronic communications networks and facilities, where there are grounds to consider that such actions are being performed and this has been claimed in writing by the affected party or a competent authority.

3. Detecting and tracking of disturbing calls, upon a request on the part of the affected subscriber claiming the undertaking providing the service to take measures.

4. Conducting market surveys, including the extent to which the provided electronic communications services satisfy the needs of users, or for the provision of value added services, requiring further processing of traffic data or location data, different from the traffic data, required for the transfer of communication or for its charging only upon end-user's prior consent.

11. According to the national rules transposing the Directive, for which purposes is data retention mandated in each case?

The retention of traffic data under the ECA is aimed at (i) detection and investigation of serious crimes, (ii) computer crimes as defined in the Bulgarian Criminal Code[7], and (iii) locating the position of individuals (Art. 250a, para 2). In

[7] Computer crimes under the Bulgarian Criminal Code may take one of the following legal forms:

(i) If a person copies, uses or gets access to computer data in a computer system without permission, if such is required (Art. 319a of the Criminal Code).

the latter case, the purpose of the ECA is to detain criminals caught in the act of performing crime (e.g. kidnapping or taking hostages). In practice, the police have already managed several times to investigate crimes committed by organised groups for kidnapping using the data retained on the ground of Art. 250, para 2 of ECA.

According to the Bulgarian legislation a "serious crime" is crime for which the Criminal Code provides for one of the following three punishments: (i) prison sentence for more than five years, (ii) life sentence with parole option, and (iii) life sentence without parole.

12. **Are there any specific rules in national law prohibiting the retention and/or transmission of sensitive data (i.e. data that is legally considered to be particularly worthy of protection, e.g. data resulting from a communication between individuals that are in a relationship of mutual trust particularly protected by law for reasons of overriding importance, as might be the case between a lawyer and his/her client, between a doctor and his/her patient, between a journalist and a whistle-blower)?**

The effective Bulgarian legislation provides for several exceptions where certain professionals are not obliged to disclose and transmit sensitive data of their clients. However, these exceptions do not prevent the competent authorities in getting access to and retaining data resulting from communications with these groups of professionals.

The Advocacy Act provides that lawyers are obliged to keep the confidentiality of their clients. Furthermore, lawyers are not allowed to act as a witness in a court of law or disseminate any information provided to him by the client in his professional capacity (Art. 45).

The Health Act imposes a special obligation to all medical staff not to disclose any health information to third parties, including data related to the health condition, the physical and mental development of individuals, as well as any other information contained in medical prescriptions, instructions, protocols, certificates and other medical documentation (Art. 28c).

(ii) If a person adds, modifies, deletes or destroys a computer system of a computer program without the permission of the person who administers or uses a computer system (Art. 319b of the Criminal Code).

(iii) If a person commits the crime under Art. 319b of the Criminal Code with respect to data, which is transferred by virtue of law, via electronic means or on a magnetic, electronic, optical or other carrier (Art. 319c of the Criminal Code).

(iv) If a person enters a computer virus into the computer system or the computer network (Art. 319d of the Criminal Code).

(v) If a person distributes passwords or user codes for access to a computer system or computer data and as a result of such distribution personal data or information representing state or other secret is disclosed (Art. 319e of the Criminal Code).

(vi) If a person while providing information services breaches the provision of Art. 6, para 2, item 5 of the Electronic Document and Electronic Signature Act (Art. 319f of the Criminal Code).

The Notary Act provides that notaries are obliged not to disclose any information, which they have acquired in the course of their duties. The non-disclosure obligation is indefinite and applies even if the person no longer occupies the position of a notary (Art. 26).

The Law on Publicity of the Property Owned by Persons Occupying High Public State Positions prohibits the disclosure of any information regarding the property and income of the relevant persons in the mass media, unless the prior written consent of the parties concerned is given (§4, Para 2 of the Transitional and final provisions).

13. **For how long do the data retained in accordance with the national rules transposing the Directive have to be kept available? In case a distinction is made according to data categories: Please describe the criteria the distinction is based upon and the reasons therefor.**

The providers of electronic communications networks and/or services are obliged to retain the data collected for a maximum period of 12 (twelve) months[8]. The data, which have already been accessed and preserved, should be retained for an additional period of 6 (six) months, if the authority that has gained the access submits a request for extension to the relevant provider.

14. **Which authorities or other bodies are entitled to access the data retained (e.g. law enforcement agencies, security authorities and/or intelligence, other public bodies, (private) claimants/litigants)?**

The Bulgarian authorities that are authorised to gain access to retained data are:

1. The specialized directorates, the territorial directorates and the stand-alone territorial departments of the State Agency for National Security.

2. The Chief Directorate Criminal Police, the Chief Directorate for Combating Organized Crime, the Chief Directorate Security Police, the Chief Directorate Border Police, the Internal Security Directorate, the Sofia Directorate of the Interior, the regional directorates of the Ministry of Interior and the territorial units of the Chief Directorate for Combating Organized Crime.

3. The Defence Information Service and the Military Police Service under the Minister of Defence.

4. The National Intelligence Service. (Art. 250b, Para 1 of the ECA)

15. **For which purposes may the data retained be used according to the national law transposing the Directive, for which purposes may they be used according to other national law (e.g. for law enforcement (criminal/administrative offences), security, civil action (e.g. to enforce copyright claims))? Does the**

[8] Art. 250a, para 1.

national law grant any rights to individuals to access the data retained directly, e.g. in a civil action (right to information on the owner of an IP address)?

The retained data can be used only for the three purposes explicitly listed in the ECA, namely: (i) detection and investigation of serious crimes, (ii) computer crimes as defined in the Bulgarian Criminal Code, and (iii) locating the position of individuals. The retained data cannot be used in civil, administrative or other as mentioned criminal proceedings or civil actions.

16. **Which specific requirements have to be fulfilled in order to access the data for one of the purposes mentioned in question 15 (e.g. a suspected serious crime, specific risks to public safety)?**

In order to gain access to retained data, the authorised competent authorities should file a reasoned request to the respective court explaining in sufficient details the motives for which such access is necessary.

17. **Is it required to obtain a court order before accessing the data retained? Is it required to hear the aggrieved party or to involve him/her otherwise in the proceedings before data is accessed?**

The access to the retained data can be granted only by a court order issued by the chairman of the respective regional court where the seat of the competent authority requesting the access is located.

The access to data concerning the president of the regional court, any ascendant, descendant, sibling, spouse or de facto cohabitee, should be addressed to the chairman of the relevant district court.

The aggrieved party is not involved in the proceedings before data is accessed. The aggrieved party is notified only afterwards.

The specialised parliamentary committee should inform the aggrieved party where any traffic data in respect of the aggrieved party has been wrongfully requested or accessed. Aggrieved parties are not informed where this will pose a risk to the attainment of the objectives of the ECA in the field of data retention (e.g. the needs of the detection and investigation of serious criminal offences and criminal offences; for tracing of persons; etc.)

18. **Is it provided for by law that the aggrieved party shall be notified of a data access? As a rule, does this notification have to be effected prior to or after the data access? Under which conditions is it allowed to deviate from this rule?**

According to the Bulgarian legislation the aggrieved party is not notified of the data access neither prior not after the data access is granted by the court.

19. Does the aggrieved party have a right to be informed about the data accessed as far as they are related to him/her?

The aggrieved party shall be informed of the data access by a special parliamentary commission only if the data access has been performed illegally. However, in such a case no notification is required if it can endanger the fulfilment of the purposes for which the data is requested.

20. May the aggrieved party have recourse to the courts for the (intended and/or already effected) data access? Which remedies do the aggrieved party dispose of? What rights does the aggrieved party have in the case of an unlawful data access or processing operation?

In case of unlawful data access or processing operation, the aggrieved party is entitled to initiate the following proceedings for protecting his/her rights, namely:

1. To request from the special parliamentary commission to impose administrative sanctions on the provider of electronic communications networks and/or services, which has failed to fulfil its obligation to ensure conditions for interception of electronic communications related to ensuring protection of personal data in the field of electronic communications (i.e. the providers failed to protect the confidentiality of the messages and the traffic data related to them, etc.). The administrative penalty may vary from BGN 2,000 to BGN 20,000.

2. To request from the special parliamentary commission to impose an administrative sanction on the person who has violated the rules regarding the protection of confidentiality of communications and the related traffic data sent over public electronic communications networks. The fine may vary from BGN 2,000 to BGN 20,000 in case the act does not constitute a criminal offence.

3. To initiate criminal proceedings against any person who has accessed, disclosed or disseminated illegally traffic data that should be collected, processed and used in accordance with the ECA. If convicted for this crime, the offender may be sentenced to imprisonment of up to 3 (three) years or be subject to probation. If the criminal offence has been committed with the purpose of gaining any profit, the imprisonment may vary from 1 (one) to 3 (three) years.

4. To initiate criminal proceedings against any person who, through a fraud or in another illegal way, uses a telecommunication network, facility or service in order to generate or divert, in his or another's interest, a directed transfer of signals, written text, images, sound, data or communications of any kind, through a conductor, radio waves, optic or other transfer medium. If convicted, the offender may be imprisoned for up to 6 (six) years and fined up to BGN 10,000. If the above-mentioned criminal act is committed (i) by two or more persons, having conspired in advance for its fulfilment, (ii) by using unregistered telecommunication device, or (iii) repeatedly, the punishment shall be imprisonment of up to 8 (eight) years and a fine varying from BGN 1,000 to BGN 5,000.

5. To initiate civil proceedings against the state for compensation of the damages (material or moral) caused by the actions or omissions of the state officials responsible for protection of the confidentiality of the retained data.

21. Are there any legal provisions protecting the data retained against unauthorised access in a particular way (not: purely technical guidelines or organisational measures, see question 40 d) in this regard)? Please describe the content of these provisions.

The entire mechanism for retention and transmission of data, including the involvement of the courts, can be considered as sufficient guarantee for prevention of unauthorised access to traffic data.

The particular safeguards preventing unauthorised access to data are contained in the procedures laid down in the ECA:

(a) The reasoned request for access to data shall be in writing and shall be drawn up by the head of the respective authority containing: (i) the legal grounds and the purpose justifying the access; (ii) the registration number of the file subject to the inquiry; (iii) the information to be included in the inquiry; (iv) the time period to be comprised by the inquiry; (v) the official that shall receive the information.

The requests by the authorities described above muts be kept in a special register, which shall not be public.

(b) The access to the requested data is provided following permission by the chairman of the district court at the seat of the authority requesting access on the basis of which an order for providing access to the data is issued. The latter order has the following mandatory contents: (i) the information to be included in the inquiry; (ii) the period of time to be comprised by the inquiry; (iii) the official to be provided the information; (iv) name, position and signature of the judge.

A special non-public register shall be kept in the district courts for the permissions or refusals that have been issued.

(c) The undertakings providing public electronic communication networks and/or services shall perform an inquiry about the requested data after submission of an access order. The submitted access order shall be entered into a special non-public register.

(d) Inquiries about the requested data in the undertakings providing public electronic communication networks and/or services may be carried out only by officials authorised in writing by the head of the undertaking.

(e) The processing of traffic data shall be carried out by officials authorised by the undertakings providing electronic communications services, who are in charge of: (i) the administration of traffic data; (ii) end-users inquiries; (iii) identification of misuse; (iv) marketing of electronic communications services; (v) provision of value

added services, requiring further processing of traffic data or location data, different from the traffic data, required for the transfer of communication or for its charging.

(f) The heads of the undertakings providing public electronic communication networks and/or services shall submit to the Communications Regulatory Commission a list indicating: (i) the current address on which to receive the order of the competent judges; (ii) the name, second name, surname and position of the authorised officials who shall receive the orders of the competent judges, as well as a telephone number to contact them; where the data is changed, the Communications Regulatory Commission shall be notified in writing within 24 hours and its chairman shall immediately make the lists available to the heads of the accessing bodies.

22. When do the accessing bodies have to destroy the data transmitted to them?

The information collected by the accessing bodies, which is not used in the institution of a pre-trial proceeding, regardless of whether the said information constitutes classified information, must be destroyed within 6 (six) months after the date of receipt. After the expiration of the said term, a formal decision for destruction of the retained data shall be taken by a three-member commission. However, the commission does not have discretionary powers to decide whether or not to destroy the retained data after the expiration of the 6-month term. The members of the commission are determined by the competent head of the relevant authority. The decision for destruction should be drawn in the form of a memorandum.

The undertakings providing public electronic communication networks and/or services, shall store for a period of 12 months the data, generated or processed in the process of their activity. The preservation for a period of up to 6 months from the date of providing information that has been accessed and stored may be required by the head of the requesting authority from the providing undertaking.

Dimension 2 (State – economy)

23. Which private bodies/enterprises (e.g. internet service providers) are obligated to retain the data? Please distinguish the group of obligated parties from providers of neighbouring services.

The obligation for data retention under the ECA applies to both public and private enterprises (Internet providers, telephone operators, etc.) without further specifying the type of undertakings it refers to. Therefore, it applies to all undertakings providing public electronic communications networks and/or services.

According to Para 1, item 50 of the Additional Provision of the ECA "*Undertaking providing public electronic communications networks and/or services* means any natural person – sole entrepreneur, or any legal person, who provides electronic communications for commercial purposes in accordance with the provisions laid down in the ECA". Outside the scope of the electronic communications services remain the information society services, which do not consist wholly or mainly in

the conveyance of signals over electronic communications networks (Para 1, item 17 of the Additional Provision of the ECA).

24. Within the group of parties obligated in principle to retain data, are there some who are (by law) or may be (upon request) exempt from these obligations, e.g. non-commercial service providers or service providers with a minor turnover/market share?

No such exceptions exist under the effective Bulgarian legislation.

25. Which of the data categories that have to be retained according to the Directive have already been retained by the obligated parties before the Directive entered into force, e.g. for billing or other business purposes or in order to comply with (other) legal obligations?

Before the Directive was transposed in the ECA and the Ordinance, the then effective Communications Act provided for an obligation of all public operators to retain data necessary only for billing purposes. The data retained should relate to information necessary for payment and preparation of bills after the end of the call or the connection till the expiry of the term during which the users may request, challenge or pay their bills.

The providers should retain billing data also on the basis of the requirements of the Bulgarian Accounting Act, which provides that data concerning the tax position of the provider (including billing data) should be stored for 5 years.

26. Are there any legal obligations on data security in place other than those mentioned in your answer to question 21 (e.g. rules on data quality, on system stability and reliability, against unauthorised destruction, loss or alteration of the data)?

The legal obligations on data security are mentioned in the Ordinance[9] and represent a complete re-write of the provisions of Art. 7 of the Directive.

27. Which additional costs (i.e. costs over and above those arising from the retention of the data categories specified in your answer to question 25) originate in total from the implementation of the national law transposing the Directive (i.e. aggregate figures of all obligated parties in your country as a whole)?

No such data has been provided by the providers or by the competent state authorities until now.

28. Do the obligated parties receive reimbursement for their costs by government? If so: Which costs are reimbursed (only costs for disclosure of retained data or also costs for investment into the required storage technology and/or costs to

[9] Art. 4.

ensure data security and separate data storage)? What legal requirements have to be met for an obligated party to be eligible for cost reimbursement?

The providers of electronic communications networks and/or services do not receive any reimbursement for the costs made by the Bulgarian state authorities.

29. What (statutory) rules are in place governing co-operation between the party retaining the data and the party (public authority) accessing them?

The providers of electronic communications networks and/or services are obligated to ensure receivability of any requests by the accessing orders 24 hours a day, seven days a week. The providers of electronic communications networks and/or services are obliged to transmit the data to the officials who requested it within the shortest possible period of time but in any case not later than 72 hours after its receipt. The Minister of Interior or officials empowered by him in writing may determine a specific time limit within which the data are to be transmitted.

After generation, the requested information should be signed by the manager of the relevant providers of electronic communications networks and/or services. The requested information should be recorded in a special register and should be transmitted to the official as designated in the request. If possible, the order of the judge and the information provided by the provider should be transmitted by electronic means in compliance with the requirements of the Electronic Government Act and the Electronic Document and Electronic Signature Act[10].

For the needs of criminal proceedings, the retained data should be made available to the court and to the pre-trial proceedings authorities under the terms and according to the procedure established by the Criminal Procedure Code.

30. Does the national law provide for any sanctions (e.g. administrative or criminal penalties) and/or obligations to pay compensation for damages suffered in case of an infringement of data retention provisions by the obligated parties? Please describe the content of these rules.

The Bulgarian legislation provides for the following administrative sanctions in case of infringement of the data retention rules by the obliged parties:

1. The aggrieved party can request from the special parliamentary commission to impose administrative sanctions on the providers of electronic communications

---

[10] Nobody except the author shall have access to the data regarding the electronic signature (Art. 14 of the Electronic Document and Electronic Signature Act).

The supplier of certification services shall not us the data kept at it for purposes different from the aims of its business activities. The supplier can disclose to third parties only the information contained in the certificates (Art. 23, para 3 of the Electronic Document and Electronic Signature Act).

The relations between the holder of the electronic signature and the supplier of certification services shall be governed by a written agreement. (Art. 23 of the Electronic Document and Electronic Signature Act).

networks and/or services, which has failed to fulfil its obligation to ensure conditions for interception of electronic communications related to ensuring protection of personal data in the field of electronic communications. The administrative penalty may vary from BGN 1,000 to BGN 10,000.

2. The aggrieved party can request from the special parliamentary commission to impose an administrative sanction on the person who has violated the rules regarding the protection of confidentiality of communications and the related traffic data sent over public electronic communications networks. The fine may vary from BGN 1,000 to BGN 10,000 in case the act does not constitute a criminal offence.

3. The aggrieved party may initiate civil proceedings against the state for compensation of the damages (material or moral) caused by the actions or omissions of the state officials responsible for protection of the confidentiality of the retained data.

4. Any official of a state body or providers of electronic communications networks and/or services who breaches the duties thereof or abuses traffic data is liable to a fine varying from BGN 1,000 to BGN 10,000, unless the act constitutes a criminal offence.

Dimension 3 (State – State)

31. Which public body is responsible for establishing the contact with the party retaining the data in order to actually access that data when an entitled body (see question 14) so wishes?

Under the applicable Bulgarian legislation, there is no centralised single point of contact that manages all data requests of public bodies to the operators/providers under the ECA. Instead, each requesting authority, after getting the required permission by the respective court, contacts directly the operators/public providers.

The requesting authorities listed by the ECA include:

1. The specialised directorates, the territorial directorates and the independent territorial units of State Agency „National Security".

2. Chief Directorate „Criminal Police", Chief Directorate „Struggle against the Organised Crime", Chief Directorate „Guard Police", Chief Directorate „Border Police", Directorate „Internal Security", the Capital Directorate of Interior, the Regional Directorates of the Ministry of Interior and the territorial units of Chief Directorate „Struggle against the Organised Crime".

3. The „Military Information" and „Military Police" services at the Minister of Defense.

4. The National Investigation Service.

The Commission for Personal Data Protection acts as a supervisory authority regarding the security of the retained data according to the ECA and the Ordinance.

Annually, not later than the 31 March, the providers of electronic communications networks and/or services should provide the Commission for Personal Data Protection, in its capacity as supervisory authority, with statistical information on (i) the cases in which data have been provided to the competent accessing authorities, (ii) the time elapsed between the initial date on which the data were retained and the date on which the competent authorities requested the transmission of the data, (iii) the cases where requests for data could not be met.

The National Assembly, acting through the above-mentioned parliamentary commission (set up on the basis of the Rules of Organization and Procedure of the National Assembly) should exercise parliamentary oversight and monitoring of the procedures for permission and implementation of access to the retained data, as well as for protection of citizens' rights and freedoms against legally non-conforming access to any such data. The parliamentary commission is entitled to:

1. Require information from the competent accessing authorities, the providers of electronic communications networks and/or services and the Personal Data Protection Commission.

2. Check the procedure and manner for retention of the data, the requests and the court orders, as well as the procedure for destruction of the data.

3. Access the premises of the competent accessing authorities and providers of electronic communications networks and/or services.

4. Prepare annual reports on the checks conducted and to propose improvement of the procedures for retention and processing of the retained data covered by the ECA.

The Personal Data Protection Commission is subordinate to the parliamentary commission at the National Assembly since the latter may exercise control and supervision on the activities of the Personal Data Protection Commission in order to safeguard the rights and freedoms of the citizens against illegal access to data.

32. Are there any regional entities (e.g. constituent states/federal states, autonomous regions or the like) vested with own authority that have been granted their own rights of access (in addition to those of the central state/federal state) to the retained data?

The regional authorities that are competent to request access to retained data are:

1. The territorial directorates and the stand-alone territorial departments of the State Agency for National Security.

2. The territorial units of the Ministry of Interior and the Chief Directorate for Combating Organized Crime.

33. What (legal) rules are in place governing co-operation among the different bodies accessing the data and between these and other public authorities (in general as well as in particular as regards the exchange of the retained data)? Have general rules of co-operation been adapted in the course of the Directive's transposition?

Annually, the Personal Data Protection Commission provides the National Assembly and the European Commission with the summarized information concerning (i) the cases in which data have been provided to the competent accessing authorities, (ii) the time elapsed between the initial date on which the data were retained and the date on which the competent authorities requested the transmission of the data, (iii) the cases where requests for data could not be met, within 2 (two) months after receipt of the said information. The summarized statistical information should not contain personal data.

Annually, not later than the 31 March, the Ministry of Interior, the Ministry of Defence, the State Agency for National Security, the National Intelligence Service and the Prosecutor General shall prepare summarized statistical information on the requests made, the court orders issued, the information on the data covered by the ECA and the Ordinance, which has been received and destroyed, and should make the said statistical information available to the parliamentary commission.

Upon ascertainment of any wrongful use, storage or destruction of the data under the ECA and the Ordinance, the parliamentary commission should notify the competent prosecuting authorities, as well as the heads of the accessing authorities and of the providers of electronic communications networks and/or services, of the violations committed. The heads of the said accessing authorities and providers of electronic communications networks and/or services are obligated to inform the parliamentary commission in due time of the measures taken to redress the violations committed.

Under the effective Bulgarian legislation, there are no special rules governing the co-operation with regard to the exchange of retained data. For instance, it is not allowed the data retained by the request of the Chief Directorate „Criminal Police" to be provided to another competent authority (e.g. Military Police Service Office at the Minister of Defense).

34. On what legal basis does the exchange of retained data with other EU Member States, other EEA Member States and (if permitted) third countries (e.g. CoE Member States party to the Cybercrime Convention) take place? Do foreign state bodies avail of a right (vis-à-vis the obligated party) to access the retained data directly? If the answer is negative: Which (national) authorities are responsible for cross-border data exchange (the conveyance of outgoing requests and the processing of (responses to) incoming requests)?

Traffic data may be made available at the request of a competent authority of another state, where so provided for in an international treaty[11] in force for the

[11] Currently, there are no such effective treaties containing rules similar to the rules for retention of traffic data contained in Directive 2006/24/EC of the European Parliament and of the Council of 15

Republic of Bulgaria. The traffic data should be accessed upon receipt of a request from a head of a chief or specialized directorate as specified by the ECA, after written permission by the chairman of the Sofia City Court or by a judge empowered by him. If the chairman of the Sofia City Court rules in favour of the request, a special order for access is issued. A special register, which shall not be open to public inspection, is kept at the Sofia City Court in respect of the permissions as granted or refused.

The competent authority of the other state should be informed of the result of the information generated on the traffic data according to the procedure provided for in the international treaty.

35. Which are the bodies in charge of monitoring compliance with the national rules (including, but not limited to, those on data security pursuant to Articles 7 and 9 of the Directive) by all parties involved? Do these authorities act with complete independence or do they exercise their functions under the supervision of a superior authority or ministry? Which kind of supervision is applied (comprehensive supervisory control in terms of both legality and technical advisability or supervision limited to the control of legality)?

In accordance with Article 9 of the Directive, the Bulgarian legislation appoints the Commission for Personal Data Protection as the national monitoring body regarding the security of retained data.

The Personal Data Protection Commission is an independent government body ensuring the protection of individuals in the processing of and access to their personal data, as well as the control on observation of the Law on Personal Data Protection. The Commission for Personal Data Protection is a public budget-supported legal entity with main office in Sofia and it shall be a first-level spender of budget credits.

In its capacity as supervisory authority, the Personal Data Protection Commission exercises supervision over the activity of the providers of electronic communications networks and/or services so as to ensure that they respect the following rules in the retention of the traffic data:

1. The retained data is of the same quality and subject to the same security and protection as those data on the network.

2. Ensuring appropriate technical and organizational measures to protect the data against accidental or unlawful destruction, accidental loss or alteration, or unauthorized or unlawful storage, processing, access or disclosure.

3. Ensuring appropriate technical and organisational measures to ensure that the data can be accessed by specially authorized personnel only.

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.

4. The data, except those that have been made available to the competent authorities and have been preserved, should be destroyed at the end of the period of retention, except in the cases expressly provided for by the law.

The Personal Data Protection Commission is an independent state body carrying out protection of the individuals in processing their personal data and in providing the access to these data, as well as the control over the observance of the Personal Data Protection Act. The Data Protection Commission is a legal entity at budget support and headquarters in Sofia.

The Data Protection Commission is a college body and consists of a chairman and 4 members. The members of the commission and its chairman shall be elected by the National Assembly upon proposal of the Council of Ministers for a period of 5 years and they can be re-elected for another mandate.

The chairman of the Personal Data Protection Commission: (i) organises and manages the activity of the commission and is responsible for the fulfilment of its obligations; (ii) represents the commission before third persons; (iii) appoints and releases the civil servants and concludes and terminates the employment contracts of the employees working under legal terms of employment in the administration of the commission.

In the cases of violation of the Personal Data Protection Act the respective individual can approach the Personal Data Protection Commission. The Personal Data Protection Commission shall take decision within 30 days which can give obligatory prescriptions to the administrator of personal data and a deadline for rectification of the offence. The commission shall send a copy of its decision to the individual. The decision of the Personal Data Protection Commission is subject to appeal before the Supreme Administrative Court within 14 days from its receipt.

As a supervisory authority the Personal Data Protection Commission supervises the activity of the undertakings providing public electronic communication networks and/or services for compliance with the following rules for retention of the traffic data in order to guarantee their protection and security. The commission shall ensure that:

1. The retained data is of the same quality and is subject to the same security and protection as the corresponding information in the network.

2. There are appropriate technical and organizational measures to protect the information of accidental or illegal destruction, accidental loss or change, or unauthorized or illegal retention, processing, access or disclosure.

3. There are appropriate technical and organizational measures to guarantee access to the data only to specially authorised staff.

4. The information, except that provided to the competent authorities and retained by them, is destroyed at the end of the retention period.

II. Relevant case-law

36. Are there any lawsuits or administrative proceedings – pending or concluded by a final adjudication – concerning the legality of the national law transposing the Directive or parts thereof?

If so, please answer to the following questions:

a) Who are the plaintiffs/claimants and the defendants/respondents?

b) Which legal norms claimed to be in conflict with the challenged law do the plaintiffs/claimants base their motion upon?

c) Please describe briefly the outcome of concluded proceedings and the essential grounds of the rulings issued. Do these rulings seek to reach a balance of the interests protected by fundamental rights and, where applicable, other norms enshrined in the constitution or having constitutional status? Do the rulings make reference to previous case-law that deals the legitimacy of other collections of personal data?

The major court case concerning retained data rules governed by the Directive dates back to March 2008. The history of the case is as follows:

On 7 January 2008 the Ministry of Interior and the State Agency for Information Technology and Communications adopted the Ordinance. Initially, Art. 5, para 1 of the Ordinance read as follows: "For the purposes of criminal investigation activities enterprises providing public electronic networks and/or services shall ensure passive technical access of the officials of the Operative-Technical Information Directorate through the computer terminal to the data retained by the enterprises".

On 19 March 2008 the non-governmental Access to Information Programme Foundation ("AIP") appealed the Ordinance before the Supreme Administrative Court ("SAC"). According to the AIP, the adoption of the Ordinance was in violation of the Constitution of the Republic of Bulgaria, the European Convention on Human Rights, and the European Union legislation. The arguments in the complaint were:

1. The adoption of the Ordinance violates the right of private life and correspondence. As set by Art. 32, para 2 of the Constitution similar provisions shall be introduced by a law – an act issued by the legislative authority. The Ordinance, however, represents a secondary legislation document.

2. The issues regarding the personal data and their technical processing, including retention and access to such data, are regulated by the Personal Data Protection Act. The ECA which entitles the Ministry of Interior and the State Agency for Information Technology and Communications to adopt the Ordinance does not contain provisions regarding the personal data. Consequently, the Ministry of Interior and the State Agency for Information Technology and Communications are not authorized to issue a regulation on retention and access to the personal data.

3. It is unacceptable that the regime of access to data qualified as personal, which is regulated by the Personal Data Protection Act, the Penal Procedure Code and the Law on Special Surveillance Devices is being changed by the Ordinance. The Ordinance provides for a "passive access through a computer terminal" of a directorate of the Ministry of Interior to all retained data, which is a drastic violation of Art. 8 of the European Convention on Human Rights.

4. The Ordinance is not in compliance with the provisions set forth by the Directive 95/46/EC and the Convention N 108 stipulating the processing of personal data and their protection.

A three-member panel of the SAC rejected the complaint with a decision as of 17 July 2008. According to the court:

1. "Passive access through a computer terminal" implies provision of access to retained data after the submission of a written request only.

2. The ECA which entitles the Ministry of Interior and the State Agency for Information Technology and Communications to adopt the Ordinance does not violate itself the Constitution, nor the Art. 8 of the ECHR.

3. The fact that the Ordinance allows for the retention of data with the purpose of revealing any kind of crimes, opposed to the stated "serious crimes" in the Directive 2006/24/EC, does not increase the scope of the Ordinance with regard to the retention of data.

4. The Regulation does not oblige for the retention of the content of messages and hence is in line with existing legislation.

This decision was appealed by the AIP. A five-member jury of the SAC as a court of final instance repealed the previous sentence and explicitly Article 5 according to the following legal reasoning: „Article 5 does not contain any restrictions as to the type of data to which access is allowed. In addition, the term "for the purposes of criminal investigation activities" is defined too broadly and there are no sufficient safeguards that Article 32 of the Bulgarian Constitution (right of inviolability of personal life) will be observed. The Ordinance does not provide any mechanism for the observance of the constitutional principle of protection against unlawful interference in the personal and family life of individuals and against encroachments on persons' honour, dignity and reputation." Article 5 does not contain sufficient measures protecting individuals against any unlawful interference in their personal and family life and therefore contravenes Article 8 ECHR, Directive 2006/24/EC and Articles 32 and 34 of the Constitution of the Republic of Bulgaria.

37. Are there any lawsuits – pending or concluded by a final adjudication – with European courts (e.g. ECtHR, ECJ) concerning the legality of data retention obligations in which your Member State is/was involved (the indication of the case number is sufficient)?

In the Georgi Yordanov v. Bulgaria Case of 24 September 2009 the ECtHR held that Art. 8 of the ECHR was violated. Sentenced to life imprisonment for aggravated murder, Mr. Yordanov complained under Article 8 (right to respect for private and family life and for correspondence) of the Convention, about the recording of a meeting with his lawyer (Application N 21480/03).

III. State of play of the application of the national law enacted to transpose the Directive

38. Where are the data stored (e.g. at the service providers' premises, with external companies, with the State)? Are the data stored locally or at a centralised level?

The providers of electronic communications networks and/or services should store the retained data in their own or leased premises.

According to the information available the providers or electronic communications networks and/or services respect their obligation to store the retained data in the specified places. From the Internet site of the parliamentary commission at the National Assembly it is evident that there are no complaints, reports or other documents indicating that the providers are in breach of the said storage obligation.

39. Are data stored outside the country or would this be permissible according to national law? If either of these cases applies: what data protection rules have the companies involved in the storage (both in your country and abroad) been obligated to?

The data should be stored on the territory of Bulgaria as the ECA does not allow data to be stored abroad.

According to the information available the providers or electronic communications networks and/or services store the retained data in Bulgaria and do not transfer it abroad. From the Internet site of the parliamentary commission at the National Assembly it is evident that there are no complaints, reports or other documents indicating that the providers are in breach of the obligation to store data in Bulgaria only.

40. Which technical and/or organisational measures ensure in practice that

a) no data are retained beyond what is permitted?

b) where so required, the necessity to obtain a court order before accessing the data is duly observed and that State bodies otherwise cannot get access to the data (e.g. technical measures inherent to the system)? Are there any

technical interfaces enabling State bodies to access the data directly (even if this may be illegal)?

c) data are not used for purposes other than those they are permitted to be used?

d) data are protected against unauthorised or unlawful (deliberate or accidental) storage, processing, access or disclosure, destruction, loss or alteration (cf. questions 21 and 26; e.g. through encryption, physical protection, application of the four-eyes principle along with secure authentication, local/decentralised storage etc)? Please describe the measures taken both by the party retaining the data and by the party accessing them.

e) data are destroyed safely (i.e. irrevocably) and immediately upon expiry of the retention period provided for by law?

f) the aggrieved parties are notified accordingly, if this is provided for by national law (e.g. technical measures inherent to the system, specific assignment of the task to staff, cf. question 18)?

g) sensitive data (cf. question 12) are not retained or transmitted, respectively, as far as this is provided for by national law?

The respective head of the authorities competent to request access to traffic data should prepare a reasoned written request for access to the traffic data stating:

1. The legal basis and the purpose for which the access is necessary.

2. The registration number of the case file for which generation of the information is necessary.

3. The data which must be entered in the information.

4. The period of time which the information should cover.

5. The designated official whereto the data are to be made available.

The accessing authorities are obliged to keep a special register, which shall not be open to public inspection, in respect of the requests made.

The court order authorising access to traffic data should mandatorily contain:

1. The data which must be entered in the information.

2. The period of time which the information should cover.

3. The designated official whereto the data are to be made available.

4. The name, position and signature of the judge.

The regional courts are obliged to keep a special register, which is not public, in respect of the permissions as granted or refused.

The providers of electronic communications networks and/or services should generate information on the traffic data after receipt of an order to provide access. Any order to provide access as received is recorded in a special register which shall not be open to public inspection.

The only officials who are empowered to generate traffic data as requested by the accessing authorities should be appointed in writing by the competent heads of the providers of electronic communications networks and/or services.

The procedures described above are laid down in the Personal Data Protection Act and Ordinance No 1 on the Minimal Level of Technical and Organisational Measures and Acceptable Level of Protection of Personal Data (promulgated in the State Gazette No 25 dated 23 March 2007). The said ordinance sets out the minimal technical and organisational measures ensuring the protection of personal data on four levels: (i) program level; (ii) physical level; and (iii) organisational level; and (iv) legislative level.

Ordinance No 1 is available on the Internet in Bulgarian language: http://www.cpdp.bg/index.php?p=element&aid=37.

41. Is there an effective control that the measures referred to in question 40 are effectively applied (e.g. data protection audit, (in-house or public) data protection officer, external auditors)?

The Law on Personal Data Protection provides that the chairman and the members of the Commission for Personal Data Protection perform preliminary, on-going and subsequent audits in accordance with the terms and conditions laid down by the Law on Personal Data Protection.

On-going audits are carried out at the request of persons concerned, as well as on the commission's initiative based on a monthly control activity plan adopted by it. Subsequent audits are carried out for implementing a decision or a compulsory instruction of the commission, and on the commission's initiative following receipt of warning about a violation. The auditors should prove their identity by their official cards and the order issued by the commission's president for the respective audit.

The audits end in a statement of findings. In cases when a violation is ascertained with the statement of findings, the latter shall be considered a statement on ascertainment of an administrative violation in the meaning of the Administrative Violations and Sanctions Act.

The detailed terms and procedure for carrying out audits are determined in an instruction of the commission.

For implementation of the monitoring activity, the Commission for Personal Data Protection is entitled to:

1. Require information from the providers of electronic communications networks and/or services.

2. Issue binding instructions, which shall be subject to immediate execution.

42. What technical (*de facto* and/or *de iure*) standards are applied with respect to data retention and transmission? Have the operational systems used been designed in such a way that interoperability is ensured? How is it ensured that security standards are adjusted to the current technological state of the art?

The technical standards that should be applied by the providers of electronic communications networks and/or services are laid down in the Ordinance. These standards repeat the provisions of Art. 7 of the Directive.

43. How is co-operation between the party retaining the data and the party accessing them effected in practice? Please describe the procedure of data transmission from the retaining to the accessing party.

In practice, the procedure for provision of retained data consists of several stages. Firstly, the competent accessing authorities file a reasoned request for access to data to the relevant regional court. If the chairman of the regional court concludes that the request is well grounded, the chairman issues a court order granting access to the requested data. The court order is entered into a special non-public register kept at the regional courts.

Once the court order is issued, the competent accessing authorities request from the providers of electronic communications networks and/or services to present them with the requested information. After the information is collected, the manager of the respective provider of electronic communications networks and/or services should sign-off the relevant requested information. The requested information should be recorded in a special register and should be transmitted to the official as designated in the request.

44. According to which procedure are cross-border requests issued or responded to, respectively? Is/are there (a) common working language(s) used in this context?

Traffic data may be made available at the request of a competent authority of another state, where so provided for in an international treaty in force for the Republic of Bulgaria. The traffic data should be accessed upon receipt of a request from a head of a chief or specialized directorate as specified by the ECA, after written permission by the chairman of the Sofia City Court or by a judge empowered by him. If the chairman of the Sofia City Court rules in favour of the request, a special order for access is issued. A special register, which shall not be open to public inspection, is kept at the Sofia City Court in respect of the permissions as granted or refused.

The working languages are Bulgarian and English.

B. National (societal) context

45. In general, is society aware of the public surveillance measures adopted in your country? How are these measures assessed by citizens, economy, the government and other public bodies? Please describe the public debate on the introduction (and, if corresponding rules have existed before the Directive entered into force, also on the amendment) of data retention in your country. Please illustrate the situation as comprehensively as possible, i.e. differentiating by political and social groups (political parties, civil rights groups, labour unions as well as other professional organisations of the professions concerned (police officers, judges, lawyers/attorneys), consumer and business associations, the media, etc), and by the parties involved (businesses, data protection officers, law enforcement agencies, government representatives).

At the time of adopting the Ordinance in 2008, the civil society and the opposition in Bulgaria expressed their disagreement with the possibility of traffic data to be eavesdropped. However, the provisions of the Ordinance were not put to public hearings. As a result, a wave of protests by citizens and non-governmental organisations swept the country. Hundreds of complaints were filed to the Ombudsman of the Republic of Bulgaria. As described above, Art. 5 of the Ordinance was eventually overruled by the Supreme Administrative Court.

The latest amendments to the ECA concerning traffic data were also subject to high public interest. As a result of numerous meetings and discussion, most of the proposals put forward by the representatives of the non-governmental organisations were approved by the Parliament.

46. Are there any obligations in your country to retain other personal data without a specific reason (e.g. passenger name records (PNRs), employment data, etc)?

Many special legislative acts provide for retention of certain personal data for the purposes of maintaining their employment records, ensuring their social security rights, pension rights, etc.

47. Are there any statistics on cases where the specific objective of a data access (e.g. the detection of serious crimes or the prevention of specific security threats) could be achieved? Are there any evaluations on the effectiveness of data retention in your country as a whole? If so: please provide the main results of the research.

Currently, there is no relevant statistics on the specific objectives of gaining data access.

48. Is there any information available about whether and, where applicable, how communication patterns have changed since data retention has been introduced in your country?

According to information published in the national press, the following statistics is available:

1. Approximately 25 request for data access are received in Sofia per day.

2. The Sofia Regional Court has issued 774 court orders in one month. The number of refusals totalled 218.

3. The Plovdiv Regional Court has issued in total 186 court orders.

There are no published reports, research materials or studies on how the relevant data retention legislation has impacted the behaviour of the customers towards using electronic communications.

49. Are there any discussions going on in your country to expand/narrow down the categories of data to be retained, their retention period or their purposes of use?

Currently, there are no ongoing discussions on the scope and categories of retention data as the legislative rules are relatively new.

C. National constitutional/legal framework

I. Dimension 1 (State – citizen)

50. Which national fundamental rights protecting privacy, personal data and the secrecy of telecommunications do exist in your country? Are there any other fundamental rights granted to citizens that could be affected by data retention (e.g. freedom of expression and information/freedom of the media, freedom of thought, religion/belief and/or conscience, judiciary basic rights, freedom of profession in cases where the confidentiality of communication is essential etc)? Do the fundamental rights mentioned result from the constitution, from other legal acts or from case-law? Please describe the scope of protection of these fundamental rights. As regards the right to secrecy of telecommunications: Which data are – according to national (constitutional) law12 – considered as telecommunications content? Is it legal under national (constitutional) law to retain this content without a specific reason?

The Constitution of the Republic of Bulgaria of 1991 sets out the fundamental citizens' rights and freedoms.

---

[12] In the following, „national (constitutional) law" means any national legal norm that (within the national legal system) is at a level superior than that of any other law (in countries with a written constitution: legal norms at constitutional level).

The privacy of citizens is inviolable. Everyone is entitled to protection against any unlawful interference in his private or family affairs and against encroachments on his honour, dignity and reputation.

No one should be followed, photographed, filmed, recorded or subjected to any other similar activity without his knowledge or despite his express disapproval, except when such actions are permitted by law (Art. 32).

The freedom and confidentiality of correspondence and all other communications shall be inviolable (Art. 34, Para 1).

The freedom of conscience, the freedom of thought and the choice of religion and of religious or atheistic views shall be inviolable. The State shall assist the maintenance of tolerance and respect among the believers from different denominations, and among believers and non-believers (Art. 37, Para 1).

No one shall be persecuted or restricted in his rights because of his views, nor shall be obligated or forced to provide information about his own or another person's views (Art. 38).

Everyone shall be entitled to express an opinion or to publicize it through words, written or oral, sound or image, or in any other way (Art. 39, Para 1).

The press and the other mass information media shall be free and shall not be subjected to censorship (Art. 40, Para 1).

Everyone shall be entitled to seek, obtain and disseminate information. This right shall not be exercised to the detriment of the rights and reputation of others, or to the detriment of national security, public order, public health and morality.

Everyone shall be entitled to obtain information from state bodies and agencies on any matter of legitimate interest to them which is not a state or official secret and does not affect the rights of others (Art. 41).

51. Under which conditions is it permitted to limit the exercise of the fundamental rights mentioned in your answer to question 50, according to national (constitutional) law?

The fundamental rights can be limited only on the basis of the following provisions laid down in the Constitution of the Republic of Bulgaria:

No one shall be followed, photographed, filmed, recorded or subjected to any other similar activity without his knowledge or despite his express disapproval, except when such actions are permitted by law.

The freedom and confidentiality of correspondence and all other communications is inviolable. Exceptions to this provision are allowed only with the permission of the judicial authorities for the purpose of discovering or preventing a grave crime.

Everyone is entitled to express an opinion or to publicize it through words, written or oral, sound or image, or in any other way. This right can not be used to the detriment of the rights and reputation of others, or for the incitement of a forcible change of the constitutionally established order, the perpetration of a crime, or the incitement of enmity or violence against anyone.

An injunction on or a confiscation of printed matter or another information medium is allowed only through an act of the judicial authorities in the case of an encroachment on public decency or incitement of a forcible change of the constitutionally established order, the perpetration of a crime, or the incitement of violence against anyone. An injunction suspension loses force if not followed by a confiscation within 24 hours.

Everyone is entitled to seek, obtain and disseminate information. This right can not be exercised to the detriment of the rights and reputation of others, or to the detriment of national security, public order, public health and morality.

Everyone is entitled to obtain information from state bodies and agencies on any matter of legitimate interest to them which is not a state or official secret and does not affect the rights of others.

52. If national (constitutional) jurisprudence has already ruled on the constitutionality/legality of the legal act(s) transposing the Directive: To which conclusion has it come? Is it possible, according to the court's opinion, to transpose the Directive in conformity with national (constitutional) law?

See the answer to question 36.

53. Does national (constitutional) law safeguard an absolute limit as to the maximum degree to which public surveillance measures collectively may restrict fundamental rights, or has an assessment/balance of interests to be carried out in each individual case?

According to the Constitution of the Republic of Bulgaria the freedom and confidentiality of correspondence and all other communications is inviolable. Exceptions to this provision are allowed only with the permission of the judicial authorities for the purpose of discovering or preventing a grave crime.

The Constitution and the ECA require that each limitation of the citizens' right of confidentiality of correspondence and communication be permitted by a court of law for each particular case. The decision of the court is based on the evidence presented, the legal ground and the aims of each particular request. Thus, the assessment in terms of the balance of interests is applied in each particular case.

54. Does national (constitutional) law require that exemptions be provided for from the obligation to retain or to transmit certain data that are worth being protected (cf. question 12)?

The national legislation does not provide for any exemptions.

II. Dimension 2 (State – economy)

55. Does the retention obligation restrict any fundamental right (e.g. professional freedom) protected by national (constitutional) law vis-à-vis the obligated parties (telecommunications and internet service providers etc)? In your opinion (based on/supported by the current state of the discussion in academia and jurisdiction, where available), are these restrictions in line with national (constitutional) law? Where are the limits to such restrictions according to national (constitutional) law?

The retention obligation does not restrict the fundamental rights of the obligated parties. However, the lack of compensation by the state to the providers of electronic communications networks and/or services creates certain tension between the state and the business.

The lack of compensation for the providers is not in compliance with the constitutional principle of free economic activity ensuring that all legal entities and individuals shall have equal legal conditions for performing business activities.

56. To what extent and under which conditions does national law allow to draw on private actors for the purpose of law enforcement or any of the other purposes of data retention (as far as provided for by the national law transposing the Directive, cf. question 11)?

The providers of public electronic communications services may collect, process and use users' data for:

1. Detecting, locating and eliminating defects and software errors in the electronic communications networks.

2. Detecting and terminating unauthorized use of electronic communications networks and facilities, where there is reason to consider that such actions are performed and this has been claimed in writing by the affected party or by a competent authority.

3. Detecting and tracing of nuisance calls, upon a request by the affected subscriber requesting that the undertaking providing the service take measures.

The providers of public electronic communications services may use the users' data for the purpose of market research, including the extent to which the electronic communications services provided by the said providers satisfy the requirements of users, or for the provision of value added services, requiring an further processing of traffic data or location data other than the traffic data necessary for conveyance of the communication or for the billing of the communication, solely where the said undertakings have obtained the consent of users. The personal data on end-users, received in connection with the research, is anonymous.

The providers of public electronic communications services have general obligation to perform their obligations under the relevant data retention legislation. If they fail to do so, sanctions varying from BGN 2,000 to BGN 50,000 may be imposed.

57. According to national (constitutional) law, is it imperative to provide for reimbursement of the obligated parties for the costs incurred?

There is no provision for reimbursement of the obligated parties for their costs.

III. Dimension 3 (State – State)

58. What status does international treaties and, in particular, the European Convention on Human Rights (ECHR) has within the hierarchy of norms of your country's legal system?

According to Art. 5, para 4 of the Constitution of the Republic of Bulgaria international treaties (including the ECHR) which are ratified in accordance with the constitutional procedure, promulgated and having come into force with respect to the Republic of Bulgaria, form part of the legislation of Bulgaria. Therefore, they have primacy over any conflicting provision of the domestic legislation, including the Constitution itself. However, in the latter case, the National Assembly shall amend the Constitution accordingly.

59. Are there any situations/configurations that might concede to Directives a particular status within the hierarchy of norms of your country's legal system and/or grant them immediate effect? In general, what steps have to be followed in order to transpose a Directive into national law in your country?

There is no legal mechanism granting EU Directives immediate or privileged effect. In general, EU Directives are implemented by the adoption of legislative acts by the National Assembly or secondary legislative acts (e.g. ordinances, regulations, etc.) adopted by the Council of Ministers or the relevant ministers and agencies.

60. Does national (constitutional) law limit the possibility of your country to transfer national sovereignties to the European Union, or does it limit the possibility for the EU to exercise competence already transferred in cases where this would be in conflict with national (constitutional) law?

No special rules regarding the transfer of sovereignty are contained in the national legislation. Art. 4, para 3 of the Constitution provides that the Republic of Bulgaria shall participate in the building and development of the European Union.

61. In which way have the powers regarding data retention been divided among ministries and authorities in your country? In case there are regional territorial entities (covering only parts of the country) that are vested with own powers and authorities (cf. question 32): how is competence split among the authorities of these entities and between these authorities and the authorities of the central state/federal state?

The agencies competent in the field of data retention are described in full in the answer to question 14 above. The competence split among the various authorities is regulated in the internal organisational acts of the various agencies and authorities.

62. Does national (constitutional) law set any limits regarding the transmission of retained data to other countries? If so: Please describe these limits.

Traffic data may be made available at the request of a competent authority of another state, where so provided for in an international treaty in force for the Republic of Bulgaria.

IV. Assessment of the overall situation

63. In your view, what options for improvement are there in your country in terms of balancing the interests of freedom and security in the context of data retention?

The main area of improvement in the area of data retention concerns the better coordination and cooperation between the Commission for Personal Data Protection and the Communications Regulation Commission. The Bulgarian society also expects that the latest changes to the ECA of 2010 will help the law enforcement authorities to fight organised crime.

Balancing the interests in the context of data retention (INVODAS)

Bulgaria

Raina Nikolova

Part 2: Overarching issues and country-specific questions

A. General part (questions to the experts in all Member States)

1. Does national (constitutional) law provide for a right to communicate *anonymously*?

The Constitution of the Republic of Bulgaria does not contain an explicit provision whereby the term "anonymous communication" is used. However, Art. 34 of the Constitution governs that the freedom and confidentiality of correspondence and all other communications shall be inviolable. Any exceptions to this rule are permitted only with the permission of the judicial authorities for the purpose of discovering or preventing a grave crime.

2. Please illustrate in detail any amendments to current data retention legislation that are presently discussed in your country. How strong (in terms of support they get by the public) are the different arguments uttered in this context? Are the proposals for improvement set out in your answer to question 63 of the first questionnaire discussed in the public? If so: by which parts of society, and what degree of attention do they get in the public debate as a whole? Particularly: is the "quick-freeze" option, as foreseen by the Council of Europe's Cybercrime Convention (Art 16 para. 2), discussed as a potential alternative to data retention?

On 11 May 2011 the Commission on Legal Matters at the National Assembly reviewed and discussed the Annual Report of the commission exercising control and monitoring for the period 20 April 2010 – 20 April 2011. The Annual Report provides comprehensive review of the application of the rules of the ECA in the field of data retention. Despite some observations and recommendations to the activities of the regional courts and prosecution offices, the specialized parliamentary commission has not made any proposals for legislative changes concerning the data retention legislation. The Annual Report also does not contain recommendation for adoption of the option set out in Art. 16, para 2 of the Council of Europe's Cybercrime Convention.

3. **In which way and to which extent are private actors (citizens, undertakings) generally obligated in your country, by means other than data retention, to co-operate with public authorities in the detection, investigation and prosecution of criminal offences and/or for any other of the legitimate purposes for which providers are (also) obligated to retain data?**

   According to Art. 159, para 1 of the Criminal Procedure Code all organizations, legal entities, officials and individuals are obliged, upon explicit order issued by the courts, the prosecutors and/or the police, to retain and deliver to the competent authorities any belongings, papers, computer information data, including traffic data, that may be relevant to a particular case.

4. **Which rules governing the rights of persons (e.g. in specific circumstances such as a lawyer) to refuse to testify/to deliver evidence against themselves (in court) do exist in the national law of your country? Do these rules include (according to their wording or according to the meaning identified through applying commonly used methods of interpretation) data that is to be retained and – as the case may be – transmitted under the national law transposing Directive 2006/24/EC on data retention (hereinafter: "the Directive")? Do these rights to refuse to testify conflict with data retention in a way that they bar these data from being retained, transmitted and/or used as an evidence in court?**

   In accordance with Art. 30, para 5 of the Constitution every citizen of Bulgaria is entitled to meet his legal counsel in private and the confidentiality of such communication is inviolable.

   The Bulgarian Criminal Procedure Code any suspected person is entitled not to give explanations and to answer questions of the prosecutors (Art. 115, para 4). In addition, the Criminal Procedure Code provides that spouse, ascendants, descendants, brothers, sisters of the accused party and the individuals with whom he/she lives together may refuse to testify.

   There are tow more rules contained in the Criminal Procedure Code providing special regulation to testifying in court: (i) witnesses are not obliged to testify on questions, the answers to which might incriminate them, their relatives of ascending and descending line, brothers, sisters, spouses or individuals with whom they live together in the commission of crime; and (ii) witnesses cannot be interrogated on circumstances were confided thereto as legal counsel.

   However, it should be clarified that the above rights to refuse to testify do not contradict to the data retention rules. Therefore, if the prosecution office or the police officers obtain traffic data on a legitimate ground from such persons, such data can be used as evidence in court.

5. **Where/how are data, that have been requested by entitled bodies, stored by these bodies once obtained? What measures have to be taken by these bodies in order to safeguard data protection and data security?**

The ECA provides that the heads of the bodies entitled to store retained data should develop internal rules and instructions governing the terms and conditions for physical storage of the retained traffic data, including their storage in separate premises in view of ensuring protection against unauthorized access. For example, the courts have developed practice to create separate desks for receiving/sending classified information.

6. **Are there any official statistics or otherwise available information on the transmission of retained data to the entitled bodies (number of requests, data categories, time period between storage and request)? If so: please attach this information or give a brief summary and indicate their source.**

The above-mentioned Annual Report of the specialized parliamentary commission contains the following statistical information. The information concerns 2010 and is divided into two:

1. For the period from 1 January 2010 till 10 May 2010:
   a. Total number of requests for access to data – 2,780;
   b. Total number of court orders providing access to data – 2,760;
   c. Total number of court orders refusing to give access to data – 20.

2. For the period from 10 May 2010 till 31 December 2010:
   a. Total number of requests for access to data – 18,934;
   b. Total number of court orders providing access to data – 18,845;
   c. Total number of court orders refusing to give access to data – 358.

The total numbers for 2010 are as follows:
   a. Total number of requests for access to data – 21,714;
   b. Total number of court orders providing access to data – 21,605;
   c. Total number of court orders refusing to give access to data – 378.

The above-mentioned information summarized in the Annual Report is based on the data collected from the annual reports of the Supreme Court of Cassation, the Supreme Prosecution Office and the Operational Technical Department at the Ministry of Internal Affairs.

B. Country-specific questions

7. **Please give your own opinion on the constitutionality of the data retention regime in your country as a whole.**

In my opinion the effective data retention regime is in compliance with the Constitution of the Republic of Bulgaria. The latter provides the opportunity for the competent authorities to limit the citizens' right of confidentiality of correspondence

and communication by using traffic data for the purpose of discovering and preventing grave crime. Therefore, the regime created by ECA is in correspondence with the above-mentioned rule (Art. 34, para 2 of the Constitution).

8. **Are the data to be retained in accordance with the Directive covered by the secrecy of correspondence, as provided for by the national (constitutional) law of your country?**

   Yes, the data retained according to the Directive are covered by the privacy of correspondence governed by the Constitution.

9. **Please explain the impact of the proportionality rule when assessing the constitutionality of a measure limiting fundamental freedoms, and what interests have to be balanced within the scope of such assessment.**

   The proportionality rule that applies to actions limiting the fundamental freedoms is laid down in Art. 6, para 2 of the Administrative Procedure Code (Any administrative act and its application should not impact any rights and legitimate interests in a manner exceeding the purpose for which the act was issued). The court practice has further developed the elements of the proportionality rule:

   a) The act should be acceptable (which means whether the action undertaken is appropriate for achieving the purpose sought),
   b) There should be proven necessity of taking the respective action (the courts are checking whether the administrative authorities have had the option to use another measure, which is less restrictive), and
   c) The severity of the measure used should correspond to the imposed restrictions.

10. **According to your answer to question 9 of the first questionnaire, in the case of pre-paid public telephone services provided through a terrestrial mobile network, Art. 251a para. 5 ECA provides that data necessary to identify the subscriber or user have to be retained. This retention obligation is not included in Art. 5 Directive 2006/24/EC. Is the legislator aware of the fact that this is a deviation from the Directive? What considerations during the legislative procedure have led to this deviation?**

    The Bulgarian legislation treats both type of mobile services (the so called pre-paid mobile services and the mobile services provided on the basis of a contract) similarly, The reason for this is that prior to the legislative changes in 2009, the pre-paid mobile services were often used by criminals for committing grave crimes (e.g. kidnapping, bomb threats, etc.).

11. **Are there any rules preventing the same data from being retained more than once (e.g. when the network operator and the service provider are different legal personalities who, in principle, would both be covered by the retention obligation)? If so: please describe the content of these rules.**

    There are no explicit rules in the effective Bulgarian legislation preventing the subsequent retention of data.

12. **Could you please provide the legal norm in the ECA prohibiting data to be stored abroad (as mentioned in your answer to question 39 of the first questionnaire)?**

    The general principle is that the ECA applies only on the territory of the Republic of Bulgaria and therefore, the storage of retained data should be performed also in the country. This rule is derived from the general rules of interpretation as there is no explicit provision to this effect.

13. **Please describe the content of Ordinance No 1. In particular: do these rules provide for measures in one or more of the following areas?**
    1. **physical protection of the data retained (e.g. through physically separated storage systems that are disconnected from the internet, located within particularly protected buildings)**
    2. **secure data storage: cryptographic security (e.g. general obligation to encrypt the data retained, possibly further detailed by specifications e.g. on the encryption algorithm to be used or on the safe custody of the crypto-keys)**
    3. **rules on internal access restriction and control (e.g. four-eyes principle, secure authenification mechanisms/certificates)**
    4. **access logging**
    5. **secure (irreversible) deletion after expiry**
    6. **error correction mechanisms (e.g. hash functions, checksums)**
    7. **secure data transmission (cryptographic security, postal delivery)**
    8. **access/request procedure (transmission by the provider on request or direct access by the entitled bodies?)**
    9. **measures to ensure that data transmitted is used exclusively for the designated purpose (e.g. tagging through electronic signature, time-stamp etc)**
    10. **staff training/internal control mechanisms to ensure compliance with the law and other rules**
    11. **measures to ensure that the principles of data reduction and data economy are respected (e.g. rules that avoid double retention of data by both the service provider and the operator of the network used for signal conveyance)**

Do the technical and organisational measures described apply specifically and exclusively to the storage and transmission of data in the context of data retention, or to any data processing (in electronic communications)?

The Ordinance provides for multiple organizational and technical measures aimed at ensuring the protection of the data retained. The measures are summarized in three groups depending on the protection level depending on the risks involved: initial, average and high.

The measures on the initial level contain the following:

1. The controller of retained data should accept security rules that are mandatory for the employees authorized with access to the data registers. These rules shall include: (i) detailed description of the data registers kept; (ii) measures at ensuring the level of security: authorized access of employees only to data and resources necessary for the performance of their duties; locking the premises; locking the cupboard/cash-box for storing the data register; (iii) rights and obligations of the employees; and (iv) procedures on reporting, management and reacting to accidents; (iv) elaborating a procedure on reporting and management of accidents (including registration of the accident, time for establishing its occurrence, the person reporting on it, the person receiving the report on it, the consequences from it and the measures for its removal).

2. The controller should also create mechanisms for preventing the access to the registers by employees outside the range of the authorized ones.

3. The information contained in the data registers should be identified, inspected and stored at place with limited access only for employees appointed by the controller. The destruction of the registers from the selected premises should be performed only by the controller or person explicitly authorized by him.

4. The controller should create archive copies and for the data restoration (the procedures for creating archive copies and for restoration of data should ensure that the data could be reconstructed in the state in which they were during their loss or destruction).

The measures at the average level are as follows (in addition to the measures at initial level):

1. The controller should create (i) rules enabling the identity of the person responsible for the security, (ii) procedures for creating archive copies and data restoration, and (iii) procedures for regular checks that should be executed in order to monitor the conformity with the rules and measures that are to be undertaken for removal of the violations.

2. The controller should create mechanisms allowing for the unambiguous, personalized identification of every employee that is trying to start up and receive access to the informational system and to establish whether every of these employees is authorized on this.

3. The controller also should set limits on the range of subsequent attempts for receiving unauthorized access to the informational system.

4. The controller should ensure that only the duly authorized employees could have access to the premises where are located the informational systems with personal data.

5. The controller must create a system for registration of the access to the data are received and/or supplied on technical carrier or via email in the local network, as it allows for the direct or indirect identification of the type of data, the date and time, the forwarding agent, the way in which the received/forwarded data were processed, as well as the receiver that should be duly authorized entity.

6. The storage of temporary files should be in conformity with the corresponding level of security and they are to be destructed immediately after the purposes for which they were created, are achieved.

7. The archive copy and the procedures for restoration of the data should be stored at different location than the place where is located the computer equipment, processing the data and in all cases there are undertaken the measures for security required for in the Ordinance.

The measures at high level of protection (in addition to the measures applicable to the initial and average levels) include:

1. The mandatory information that should be registered at high level of protection is: identity of the employee; date of accessing; the register for which access was granted; the type of access and when access was denied.

2. The controller should register the information that allows for identifying the entry to which the employee had access.

3. The above information must be stored for a period of at least two years.

4. The rules for registering the above-described data should be set out that the controller in person or via person appointed personally by him executes the control on their respecting and for not allowing their deactivation.

5. The controller is liable for the execution of regular checks on the recorded information on the control and prepares report on them, established at least once monthly.

6. The controller should provide additional measures in connection with encryption or utilization of the data retained ensuring that the data are not readable or they were not modified.

The measures set out in the Ordinance apply to data processing in general and not only specifically for the purpose of the data retention regime.

14. **Please provide the legal and/or technical/organisations where the rules for co-operation between the party retaining the data and the party (public authority) accessing them (see your answer to questions 29 and 43) and among the different bodies accessing the data and between these and other public authorities (see your answer to question 33) are laid down.**

The following co-operation rules exist:

1. The heads of the undertakings providing public electronic communications networks and/or services shall transmit to the Communications Regulation Commission special lists containing the following information: (i) the current address for receipt of the court orders allowing/refusing access to traffic data; (ii) the forenames, patronymics, surnames and position of the officials empowered to receive the court orders

2. Annually, not later than the 31st day of March, the undertakings providing public electronic communications networks and/or services shall provide the Commission for Personal Data Protection, in its capacity as supervisory authority, with statistical information on: (i) the cases in which data have been provided to the competent authorities; (ii) the time elapsed between the initial date on which the data were retained and the date on which the competent authorities requested the transmission of the data; (iii) the cases where requests for data could not be met.

3. Annually, the Commission for Personal Data Protection shall provide the National Assembly and the European Commission with the summarized information described in item 2 above within two months after receipt of the said information.

15. **Your answers to questions 34/44 of the first questionnaire seem to cover exclusively the situation that a non-EU Member State files a data request. Please explain the legal basis and the practical procedure in case of a request for retained data made by an authority from another EU Member State.**

The ECA does not treat differently the EU Member States from the non-EU Member States. Art. 251 of the ECA is in direct correlation with Art. 15, §1 of Directive 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).

16. **Supervisory bodies:**

a) **Please explain the role of the "special parliamentary commission" in relation to the Commission for Personal Data Protection. How can the respective tasks of the two bodies be delimited against each other?**

As mentioned above, annually, the Commission for Personal Data Protection shall provide the National Assembly with a summary of the information mentioned in Answer 14, item 2 above within two months after receipt of the said information.

b) Which authorities are in charge of monitoring compliance of the providers with the data retention obligations, as far as these obligations do not explicitly refer to the protection of personal data (e.g. the obligation to retain the data etc)? Are these supervisory bodies independent in the sense of what has been said in question 35 of the first questionnaire?

The competent authority is the Communications Regulation Commission, which has powers to monitor the compliance of all providers with data retention obligations (including obligations outside the personal data protection. The Communications Regulation Commission is independent in the meaning of Question 1 of the first questionnaire.

c) Are there any external bodies responsible for supervising that the bodies entitled to obtain access to the data retained (police etc) act within the law? Are these supervisory bodies independent in the sense of what has been said in question 35 of the first questionnaire?

No such specialized external bodies exist.