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

Cyprus

Olga Georgiades

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.

  Comment by the author:

  Prior to the enactment of the *Retention of Telecommunications Data for the Purpose of Investigating Serious Criminal Offences Law of 2007 (N. 183(I)/2007)* (hereinafter "the Data Retention Law") which transposed the Directive 2006/24/EC (hereinafter "the Directive"), there was no specific legislation concerning the retention of electronic communications data which would compel communications Service Providers to routinely capture and archive information detailing the telephone calls, e-mail messages and other communications of their users for specific periods of time (i.e. 6 months).

  Nevertheless, it should be noted that the Regulation of Electronic Communications and Postal Services Law of 2004 as amended (hereinafter the "Electronic Communications Law") which was enacted before the adoption of the Data Retention Law contains extensive specific provisions regarding the power and competence of the Regulator of Electronic Communications to obtain information by:

(a) Demanding that electronic communications network and/or electronic communications and/or postal Service Providers provide such information and submit statements and reports in relation to their operations at such intervals and in such form, as the Commissioner may from time to time prescribe; and

(b) Ordering any person to provide such information.

In addition, the Law for the Protection of Privacy of Private Communication (Monitoring Communications) of 1996, Law N. 92(I)/1996 (hereinafter the "Data Protection Law"), which is still in force, allowed, under certain conditions, for, inter alia:

(a) The monitoring of private communications,

(b) The recording of telephone call numbers for billing purposes,

(c) The monitoring of the content of a private communication made with prisoners,

(d) The monitoring of private communications by the Cyprus Telecommunications Authority where this is accidental or absolutely necessary for the purpose of providing telecommunications services or for maintaining or ensuring quality of telecommunications equipment.

Finally, it should also be noted that certain legal provisions were in place before the enactment of the aforementioned law in the field of banking concerning, inter alia, the retention of data for uncleared banking cheques in electronic form (*Central Information Register for Uncleared Cheques Order of the Central Bank of Cyprus of 2002*). In addition, the Taxation Law provides for the retention of certain data for a five year period but such data do not concern electronic communications data.

- *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 Directive was transposed by the *Retention of Telecommunications Data for the Purpose of Investigating Serious Criminal Offences Law of 2007*, N. 183(I)/2007 (*Ο Περί Διατήρησης Τηλεπικοινωνιακών Δεδομένων με Σκοπό τη Διερεύνηση Σοβαρών Ποινικών Αδικημάτων Νόμος του 2007)*.

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

  Not applicable

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 English version available.

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

   The Data Retention Law was published in the official Gazette of the Republic on 31/12/2007 and entered into force on that date. The Data Retention Law was amended in 2008 by Amending Law N. 99(I)/2008.

   It should be noted that the Republic of Cyprus postponed the application of the Directive and the Data Retention Law to the retention of communications data relating to Internet Access, Internet telephony and Internet e-mail pursuant to Article 15(3) of Directive. The Data Retention Law regulates the terms under which the retention of personal data for the purpose of crime investigation, detection and prosecution is legal.

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

The type of legal act is a Law enacted by the House of Representatives of the Republic of Cyprus.

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**

   The secondary legislative instruments in place are in the form of an Order of the Council of Ministers which deals with more technical/technology-oriented provisions. Namely, this is the Retention and Processing of Traffic Data Order of 2007.

   This Order was issued by virtue of the Regulation of Electronic Communications and Postal Services Law of 2004 as amended for the purpose of harmonisation with Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications). This Order was issued on 28 December 2007.

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.**

   The type of legal act chosen, namely the primary Law, is usually adopted for the purpose of prescribing the general framework regulating a matter which is the subject matter of the legislation. Generally, Regulations or Orders are adopted on the basis of the Data Retention Law in order to implement the provisions of the Law in practice or to prescribe more detailed provisions and to deal with more technical/technology-oriented provisions. Regarding the particular Law under consideration, section 21 provides that the Council of Ministers may issue Regulations prescribing the details relevant to the maintenance of statistical data as well as any other matter deemed necessary for the purpose of the optimal implementation of this Law.

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?**

   The terms defined in Article 2 (2) of the Directive are also defined within the Data Retention Law which transposes the Directive.

The following is a comparison of the definitions of the Directive and the Data Retention Law:

Directive	Cyprus Law
"Data" means traffic data and location data and the related data necessary to identify the subscriber or user.	"Data" means traffic data and location data and the related data necessary to identify the subscriber and/or user and which are prescribed in sections 6, 7, 8, 9, 10 and 11 of this Law.
"User" means any legal entity or natural person using a publicly available electronic communications service, for private or business purposes, without necessarily having subscribed to that service.	Exactly same text
"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).	Exactly same text
"User ID" means a unique identifier allocated to persons when they subscribe to or register with an Internet access service or Internet communications service.	Exactly same text
"Cell ID" means the identity of the cell from which a mobile telephony call originated or in which it terminated.	Exactly same text
"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.	The exact translation of the relevant definition from the Greek "unsuccessful call" and not "unsuccessful call attempt" but the remainder of the definition is practically the same.

There are certain additional definitions provided, namely, "Police", "Police investigator", "Judge", "Court", "Service Provider" and "Serious criminal offence".

The Data Retention Law provides that for the purposes of this Law the terms used therein and not prescribed in this Law shall have the meaning ascribed thereto by the Law for the Processing of Personal Data (Personal Protection) and the Regulation of Electronic Communications and Postal Services Law. These Laws had the purpose of harmonising Cypriot legislation with Directives 95/46/EC, 2002/21/EC and 2002/58/EC.

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?

According to section 3 of the Data Retention Law, the data to be retained are those generated or processed by providers of publicly available electronic communications services or of a public communications network including fixed and mobile telephony within the framework of the process of supplying the communications services concerned (the Service Providers).

According to the Cyprus Law, "Data" is defined as traffic data and location data and the related data necessary to identify the subscriber and/or user prescribed in sections 6, 7, 8, 9, 10 and 11 of the Law. These sections define the categories of data to be retained:

(a) data necessary to trace and identify the source of a communication

(b) data necessary to identify the destination of a communication

(c) data necessary to identify the date, time and duration of a communication

(d) data necessary to identify the type of communication

(e) data necessary to identify users' communication equipment or what purports to be their equipment

(f) data necessary to identify the location of mobile communication equipment

The law does not go beyond the obligations mentioned in the Directive because it reproduces the wording used by the Directive.

The obligation to retain data includes the retention of the data relating to unsuccessful call attempts but does not extend to the retention of data relating to calls not connected to the destination number.

The Retention and Processing of Traffic Data Order of 2007 also applies with regards to the retention of traffic data of subscribers and users of providers of fixed and mobile telephony.

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 Retention and Processing of Traffic Data Order of 2007 also applies with regards to the retention of traffic data of subscribers and users of providers of fixed and mobile telephony for the purpose of charging for services, payment of subscriptions and dispute resolution in relation to connection or billing. This Order was adopted for the purposes of harmonisation with Directive 2002/58/EC and as a result it may be considered to go beyond the provisions of Directive 2006/24/EC.

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

The purposes for retaining data are the following:

(a) For tracing and identifying the source of a communication.

Concerning fixed network telephony and mobile telephony, the purpose is to trace and identify (i) the calling telephone number and (ii) the name and address of the subscriber or registered user. Concerning Internet e-mail and Internet telephony the purpose is to trace and identify (i) the user ID(s) allocated, (ii) the user ID and telephone number allocated to any communication entering the public telephone network and (iii) the name and address of the subscriber or registered user to whom an Internet Protocol (IP) address, user ID or telephone number was allocated at the time of the communication.

(b) For identifying the destination of a communication.

Concerning fixed network telephony and mobile telephony the purpose is to identify (i) the number(s) dialled (the telephone number(s) called), and, in cases involving supplementary services such as call forwarding or call transfer, the number or numbers to which the call is routed and (ii) the name(s) and address(es) of the subscriber(s) or registered user(s);

Concerning Internet e-mail and Internet telephony the purpose is to identify (i) the user ID or telephone number of the intended recipient(s) of an Internet telephony call and (ii) the name(s) and address(es) of the subscriber(s) or registered user(s) and user ID of the intended recipient of the communication.

(c) For identifying the date, time and duration of a communication:

Concerning fixed network telephony and mobile telephony, the purpose is to identify the date and time of the start and end of the communication.

Concerning Internet access, Internet e-mail and Internet telephony, the purpose is to identify (i) 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 registered user and (ii) the date and time of the log-in and log-off of the Internet e-mail service or Internet telephony service, based on a certain time zone.

(d) For identifying the type of communication:

Concerning fixed network telephony and mobile telephony, the purpose is to identify the telephone service used. Concerning Internet e-mail and Internet telephony, the purpose is to identify the Internet service used.

(e) For identifying users' communication equipment or what purports to be their equipment:

Concerning fixed network telephony, the purpose is to identify the calling and called telephone numbers. Concerning mobile telephony, the purpose is to identify

(i) the calling and called telephone numbers,

(ii) the International Mobile Subscriber Identity (IMSI) of the calling party;

(iii) the International Mobile Equipment Identity (IMEI) of the calling party;

(iv) the IMSI of the called party;

(v) the IMEI of the called party;

(vi) In the case of pre-paid anonymous services, the date and time of the initial activation of the service and the location label (Cell ID) from which the service was activated.

Concerning Internet access, Internet e-mail and Internet telephony, the purpose is to identify (i) the calling telephone number for dial-up access and (ii) the digital subscriber line (DSL) or other end point of the originator of the communication.

(f) **For identifying the location of mobile communication equipment such as** the location label (Cell ID) at the start of the communication;

(g) **For identifying the geographic location of cells by reference to their location labels (Cell ID) during the period for which communications data are retained.**

According to the Data Retention Law, an order may be issued by the Court enabling a police investigator to obtain access to data which are related to a serious criminal offence, in order to obtain evidence that a serious criminal offence has been committed. The term serious criminal offence is defined as a crime for which a prison sentence exceeding five years is imposed in accordance with the Criminal

Code or any other applicable law. Criminal offences can be determined by any law applicable in Cyprus, depending on the subject and not specifically an offence committed for breach of this Law. For instance, criminal offences are defined in the Criminal Code but there are innumerable laws providing for criminal offences and cannot be mentioned here. The classification of a serious crime depends on the duration of the prison sentence imposed by the specific law. When a prison sentence exceeds 5 years then the criminal offence is considered serious. If an offence is serious because it exceeds a prison sentence of 5 years, then it is required that a police investigator request an order by the Court in order to obtain access to the data needed for proving a criminal offence.

The purposes for retaining data mentioned below under the answer to question 15 are also purposes for retaining data.

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)?**

There are no specific provisions in the Data Retention Law with regards to sensitive data. In any event, the Data Retention Law prescribes that the content of the relevant communication may not be disclosed in accordance with the Processing of Personal Data (Personal Protection) Law which contains specific rules regarding the processing of sensitive data. Cyprus Law does not recognise doctor - patient, journalist - whistle-blower privilege. The Advocates Law recognises lawyer-client privilege. In any event, the Constitution and the Protection of Privacy of Private Communications (Monitoring Communications) of 1996, Law N. 92(I)/1996 contain provisions regarding the tapping and use of private communication or privileged communication in the event of serious offences for the gathering of evidence. Any type of data can be retained and used as evidence for this purpose.

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 duration of the obligation for data retention is six (6) months with regards to all categories of data (section 13 of the Data Retention Law), namely data related to fixed telephony, mobile telephony, the Internet and email. Nevertheless, in accordance with section 18 of the Data Retention Law, the Council of Ministers may extend the period for the retention of the data for further six (6) month periods in the event of a declaration of an emergency situation.

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 bodies entitled to access the data retained are police investigators obtaining approval from the Attorney General of the Republic and on the basis of this approval file an application for the issuing of a Court order from the competent Court.

In addition, the Data Protection Commissioner established by virtue of the Processing of Personal Data (Personal Protection) Law also has access to such data because it acts as the Supervising Authority.

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 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 data retained is to be used by the police and the attorney general's office for law enforcement purposes in investigating and prosecuting serious criminal offences. Serious criminal offences in any field, e.g criminal offences prescribed by the Criminal Code. The data retained are not to be used for civil law claims and cannot be accessed directly by individuals in a civil action.

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)?

A serious criminal offence has been committed, is being committed or it is expected to be committed. There must be reasonable suspicion or possibility that a person is committing, has committed or is expected to commit a serious criminal offence or there is reasonable submission or possibility that specific data is connected or is relevant to a serious criminal offence.

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?

A court order must be obtained before accessing the data. There is no requirement to hear the aggrieved party or to involve him in the proceedings at the time that the Court is about to decide whether to issue the Court order.

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?

In accordance with the provisions of the Data Retention Law, prior to data access, there is no requirement to hear the aggrieved party or to involve him in the proceedings at the time that the Court is about to decide whether to issue the Court order. After data access there is no such requirement for notification of the aggrieved party either.

It should be noted that the Protection of Privacy of Private Communications (Monitoring Communications) of 1996, Law N. 92(I)/1996, contains provisions regarding the notification of persons regarding the issuing of a Court order and other relevant information regarding the carrying out of the tapping of private communication carried out through telecommunications means. This Law specifically applies to the tapping of private communications and contains provisions outlining which data may be tapped or not. It does not contain any procedures for the manner in which data is to be retained.

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

In general, a data subject has a right to be informed about any processing of data about him/her in accordance with the provisions of the Processing of Personal Data (Personal Protection) Law (right of information).

Processing according to the Data Protection Law includes the collection, recording, organization, preservation, storage, alteration, extraction, use, transmission, dissemination or any other form of disposal, connection or combination, blocking, erasure or destruction of personal data. In addition, every person has the right to know whether the personal data relating to him are or were processed (right of access).

Despite the existence of the above rights of information and access, the Data Protection Law provides that the obligation to inform may, on the application of the controller, be waived wholly or partly, by decision of the Data Protection Commissioner where the collection of personal data is performed for the purposes of defence, national needs or national security of the Republic or for the prevention, detection, investigation and prosecution of criminal offences. Where access is concerned, by a decision of the Data Protection Commissioner, on application by the controller, the obligation to inform may be waived, wholly or partly, where the processing of personal data is performed for purposes relating to national needs or to the national security of the Republic or for the prevention, investigation, detection and prosecution of criminal offences.

It follows from the above that although there is a general right of information and access, this may be waived in the events described above.

The Data Retention Law does not contain any provisions regarding any right of information as to the data accessed.

It should be noted that the Protection of Privacy of Private Communications (Monitoring Communications) of 1996, Law N. 92(I)/1996, contains provisions regarding the notification of persons regarding the issuing of a Court order and other relevant information regarding the carrying out of the tapping of private communication carried out through telecommunications means.

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?

The Data Retention Law does not contain any relevant provisions regarding the aggrieved party's right to have recourse to the courts for the (intended and/or already effected) data access. The rights of an aggrieved party in the case of an unlawful data access or processing operation by virtue of the Data Retention Law (section 16) is the right to compensation in accordance with the provisions of section 17 of the Data Protection Law. According to that section, the controller shall compensate a data subject who has suffered damage by reason of violation of any provision of the Data Protection Law, unless he proves that he is not responsible for the event that caused the damage.

It should be noted that the Protection of Privacy of Private Communications (Monitoring Communications) of 1996, Law N. 92(I)/1996 contains specific provisions regarding the right of the aggrieved person to have recourse to the Courts with regards to Court orders issued under the said Law.

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 Data Retention Law provides for the Confidentiality and security of processing of personal data in accordance with the provisions of the Data Protection Law and the Regulation of Electronic Communications Law (section 14).

Service Providers are subject to an obligation to:

(a) Ensure that the retained data shall be of the same quality and subject to the same security and protection as those data on the network;

(b) Protect the retained data by taking appropriate technical and organisational measures against accidental or unlawful destruction, accidental loss or alteration, or unauthorised or unlawful storage, processing, access or disclosure;

(c) Ensure that only specially authorised personnel can have access to the retained data and keep a register of authorized personnel as well as a register where all

access of authorized personnel to retained data shall be recorded, as well as the date and time and purpose of access;

(d) Destroy the data at the end of the period of retention, except those that have been ordered by the Court to be accessed and ordered to be preserved separately.

The Data Retention Law also refers to the protection of privacy of personal communications (section 22 of the Data Retention Law) in accordance with the provisions of the Protection of Privacy of Personal Communications Law. Finally, it is a criminal offence for any person to gain access to retained data without a valid Court order or to disclose data which he became aware of to any third parties regarding the procedure for the investigation of a serious crime.

It should be noted that the Protection of Privacy of Private Communications (Monitoring Communications) of 1996, Law N. 92(I)/1996 also contains specific provisions regarding the safe keeping of private communications carried out through telecommunications means.

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

According to section 22 of the Data Retention Law, when it is ascertained with the consent of the Attorney General that the data obtained on the basis of a Court order are not connected to the commission of a serious criminal offence for which the order was issued, shall be destroyed within 10 days from the day that the Attorney General notifies his consent; the Supervising Authority shall be notified of the above.

The Data Protection Law also provides that data must be destroyed if their processing (including their retention) is no longer necessary.

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 obligated parties are all "Service Providers" (hereinafter the "Service Providers"), that is, according to the definition provided in section 2 of the Data retention Law, providers of publicly available electronic communications services or of a public communications network including fixed and mobile telephony.

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?

The obligated parties are all Service Providers (as the term is defined in section 2 of the Data retention Law). The Data Retention Law does not contain any provisions exempting any Service Provider irrespective of their size or turnover.

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?

By virtue of the application of the provisions of the Law for the Protection of Privacy of Private Communications (Monitoring Communications) of 1996, Law N. 92(I)/1996, the data categories retained before the Directive entered into force are:

(a) The contents of private communications carried out through telecommunications.

(b) Numbers of telephone calls for billing purposes.

A Constitutional amendment in 2010 provides that the Attorney General can authorize phone tapping. The amendment also allows the police to monitor web logs, downloads and emails as admissible evidence for criminal investigations.

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)?

There are no other legal obligations on data security in place.

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 additional costs are known or mentioned in the relevant legislation.

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 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 Data Retention Law does not contain any provisions regarding the reimbursement of costs by the government.

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

According to section 5 of the Data Retention Law, where a Service Provider is presented with a data access order issued by the Court has an obligation to make available immediately and in any event without undue delay all data prescribed in the relevant Court order to the Police investigator.

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.

Where sanctions are concerned, where a Service Provider violates the provisions of the Data Retention Law, it shall be guilty of an offence and shall be liable on conviction to imprisonment for up to 3 years or to a fine of up to EUR17, 000 or to both such sanctions. In the event of a repeated violation, the Service Provider may be subject to the issuing of a Court order ordering that the Service Provider's license to operate be revoked.

Where a person discloses the contents of a communication such person shall be liable to imprisonment for a period of up to five years or to a fine of up to 25,000 Euros or to both.

Where a person is acting under the authority of the investigating organ and acquires or attempts to acquire access to retained data without a Court order or notifies the data which he has gained knowledge of to third parties or makes any changes to such data which he gained access to, he shall be liable to imprisonment for a period of up to five years or to a fine of up to 25,000 Euros or to both.

In addition to the above, the Data Retention Law appoints the Data Protection Commissioner as the Supervising Authority for the purpose of monitoring the application of the provisions of this Law. The Supervising Authority has the following powers:

(a) Carry out examinations, to examine complaints and impose administrative fines by virtue of the Data Protection Law on data processors regarding violations of the Data Retention Law;

(b) In the event of possible prima facie violation consisting in a criminal offence by virtue of the provisions of the Data Retention Law, submit information which it has at its disposal before the Attorney General of the Republic who shall decide whether there is any criminal liability justifying criminal prosecution of the offender.

(c) Deal with the case herself and impose any sanctions foreseen by the Data Protection Law which are suitable in her opinion.

With regards to compensation, an aggrieved party, in the event of an unlawful data access or processing operation by virtue of the Data Retention Law (section 16) has the right to compensation in accordance with the provisions of section 17 of the Data Protection Law. According to that section, the controller (in this case the Service Provider) shall compensate a data subject who has suffered damage by reason of violation of any provision of the Data Protection Law, unless he proves that he is not responsible for the event that caused the damage.

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?

The public body responsible for establishing such contact is the Police Investigator. The Data Retention Law defines this term as a member of the police who is investigating a serious crime and/or any other person authorized to carry out investigations for the purpose of investigating a serious crime in accordance with the provisions of section 4 of the Criminal Procedure Law.

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?

There are no such regional entities as the Republic of Cyprus has a centralised government.

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?

The Data Retention Law does not contain any other specific rules regarding the cooperation between the Police Investigator and the Service Provider retaining the data, other than those rules set out in the reply to question 29 above.

With regards to the cooperation between public authorities themselves, the said Law contains a rule that the Police Investigator needs to file an application to the Attorney General in order for the latter to approve the application for the issuing of a Court order.

The Attorney General needs to be satisfied that the issuing of the Court order is capable of providing evidence regarding the commission of the serious criminal offence. The aforementioned application to the Attorney General must be made in writing and must have as attachment an affidavit of the Police Investigator containing certain information enumerated in section 4 of the Law. After approval of the application by the Attorney General, an application is filed before the competent Court for the issuing of a court order authorizing access to the data.

Finally, the Data Retention Law appoints the Data Protection Commissioner as the Supervising Authority for the purpose of monitoring the application of the provisions of this Law. The Supervising Authority has the following powers:

(a) Carry out examinations, to examine complaints and impose administrative fines by virtue of the Data Protection Law on data processors regarding violations of the Data Retention Law;

(b) In the event of possible prima facie violation consisting in a criminal offence by virtue of the provisions of the Data Retention Law, submit information which it has at its disposal before the Attorney General of the Republic who shall decide whether there is any criminal liability justifying criminal prosecution of the offender.

(c) Deal with the case herself and impose any sanctions foreseen by the Data Protection Law which are suitable in her opinion.

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)?

The Republic of Cyprus, by virtue of ratifying Law N. 25(III)/2004 ("the Ratifying Law"), has ratified the Convention established by the Council in accordance with Article 34 of the Treaty on European Union, on Mutual Assistance in Criminal Matters between the Member States of the European Union (OJ C 197, 12.7.2000, p. 3) as well as its Protocol.

With regards to Article 18 (Requests for interception of telecommunications) and Article 19 of the Treaty (Interceptions of telecommunications on national territory by the use of Service Providers), the Ratifying Law provides that the provisions of the Protection of Privacy of Private Communications (Monitoring Communications) of 1996, Law N. 92(I)/1996, shall apply. With regards to the application of Article 20 of the Treaty (Interception of telecommunications without the technical assistance of another Member State), the Ratifying Law provides that the provisions of the Data Protection Law shall apply.

The competent authorities for the purposes of implementation of the Treaty and its Protocol are the Courts having criminal jurisdiction, the Attorney General of the Republic, the Ministry of Justice and Home Affairs, the Chief of Police, the Director of Customs, the Director of Inland Revenue, the Data Protection Commissioner, the Unit for Anti-Money Laundering, the Central Bank of Cyprus, criminal investigators appointed by the Council of Ministers in accordance with the Criminal Procedure Law.

With regards to CoE members, the Law Ratifying the Cybercrime Convention of 2004 N. 22(III)/2004 as amended, provides that for the purposes of mutual assistance the Ministry of Justice and Home Affairs shall be the central authority for the purposes of Article 17 of the Convention (Expedited preservation and partial disclosure of traffic data).

According to section 18 of the aforementioned ratification law, for the purposes of Article 35 of the Convention (24/7 Network), the Cyprus Police is the designated Point of Contact available on a twenty-four hour, seven-day-a-week basis, in order to ensure the provision of immediate assistance for the purpose of investigations or proceedings concerning criminal offences related to computer systems and data, or for the collection of evidence in electronic form of a criminal offence.

With regards to third countries, the Republic of Cyprus has also ratified the Instrument (the "Instrument") as contemplated by Article 3(2) of the Agreement on Mutual Legal Assistance between the United States of America and the European Union signed on 25 June 2003, as to the application of the Treaty (the "Treaty") between the Government of the United States of America and the Government of the Republic of Cyprus on Mutual Legal Assistance in Criminal Matters signed 20 December 1999.

In accordance with the above Instrument, the Parties shall provide mutual assistance in accordance with the provisions of the Treaty in connection with the investigation, prosecution and prevention of offences and in proceedings related to criminal matters. Mutual legal assistance shall also be afforded to a national administrative authority investigating conduct with a view to criminal prosecution. Assistance shall include, inter alia, providing documents, records and other items, locating or identifying persons or items and executing searches and seizures. The Treaty also provides for the search and seizure of items.

Foreign state bodies do not have the right (vis-à-vis the obligated party) to access the retained data directly but they need to make an application to the competent authorities described above.

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)?

The Data Retention Law (section 15) appoints the Data Protection Commissioner as the Supervising Authority for the purpose of monitoring the application of the provisions of this Law. The Supervising Authority has the following powers:

(a) Carry out examinations, to examine complaints and impose administrative fines by virtue of the Data Protection Law on data processors regarding violations of the Data Retention Law;

(b) In the event of possible prima facie violation consisting in a criminal offence by virtue of the provisions of the Data Retention Law, submit information which it has at its disposal before the Attorney General of the Republic who shall decide whether there is any criminal liability justifying criminal prosecution of the offender.

(c) Deal with the case herself and impose any sanctions foreseen by the Data Protection Law which are suitable in her opinion.

The Law specifically provides that the Supervising Authority acts with complete independence when exercising its aforementioned duties.

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?

Only one civil case has been located regarding the issuing of an Order of Certiorari dated 21/01/2010, Case No 1/2010. The case title is as follows:

"Application of Andreas Alexandrou for permission of the Supreme Court to file an application for the Issuing of an Order of Certiorary by virtue of Article 155 of the Constitution and sections 3 and 9 of the Award of Justice (Miscellaneous Provisions) Law of 1964 and Articles 1A, 15, 17 and 30 of the Constitution, Law 183(I)/2007 and Directive 2006/24/EC and with respect to the Order for the Disclosure of Telecommunications Data issued by the District Court of Nicosia on 5/8/2009."

The case is not subject to appeal because the decision was adopted by the Supreme Court (the highest court of the Republic) and has not been appealed.

If so, please answer to the following questions:

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

The claimant is Andreas Alexandrou. There is no respondent because the case concerns the annulment of a decision of the District Court of Nicosia.

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

The case concerned the claim that the Court Order was issued in excess of jurisdiction in view of the fact that the provisions of the Data Retention Law were not covered by the provisions of Article 1A of the Constitution because the Law was erroneously adopted for the purpose of preservation of telecommunications data for the purpose of investigation of criminal offences and was thus contrary to the provisions of Directive 2006/24/EC by virtue of which the data Retention Law had been adopted. The lawyer of the applicant referred to the scope/purpose of the Directive as set out in the decision of the European Court of Justice in the case Ireland v. European Parliament and Council of the European Union, Case no. C301/06 dated 10.2.09, which explained the scope/purpose of the Directive.

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 Supreme Court decided that the lifting of the confidentiality of telecommunications data was contrary to fundamental right established by Article 17 of the Constitution (Right of Privacy of Communications). The violation of constitutional provisions consists in excess of competence and a Court decision issued in excess of competence lacks competence. The Supreme Court also decided that the Retention of Data Law does not contain any provisions for the right to appeal and as a result, on the basis of established case law, this provided a right for the filing of an application for the issuing of an order of certiorari in order to examine the compatibility of the order issued by the Court of First Instance with Articles 15 and 17 of the Constitution.

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)?

No such cases are known.

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?

- ***Service Providers:***

According to section 3 of the Data Retention Law, Service Providers have an obligation to retain the data generated or processed by them within their jurisdiction in the process of supplying the communications services concerned. Other than that general obligation imposed on the Service Providers, the Law does not specify where such data need to be stored.

The Data Protection Law provides that its scope of application concerns data by a controller established in the Republic or in a place where Cyprus law applies by virtue of public international law or by a controller not established in the Republic who, for the purposes of the processing of personal data, makes use of means, automated or otherwise, situated in the Republic. It follows that if a data controller (in this case a Service Provider) is not established in Cyprus ***and*** the data is not stored in Cyprus, then a Service Provider may not be considered to be under the scope of application of the Law.

The Data Protection Law also provides that is a Service Provider is using the services of a third party to store the data there must be a written contract between the Service Provider and a data processor.

- ***The State:***

  By virtue of the provisions of section 20 of the Data Retention Law, the State may also engage in the storing of data after an access order is issued by a competent Court. In this respect, the Police Investigator will be deemed to be storing data accessed as evidence on the basis of the said access order until the completion of the investigation and the completion of the procedure before the Court handling a case.

  The Protection of Privacy of Private Communications (Monitoring Communications) of 1996, Law N. 92(I)/1996, section 13, provides that where the content of any private communication has been collected by the Police following a valid court order, such content must be stored in a safe manner by the Police. After the expiration of the court order, the stored content of the communication must be made available to the Attorney General who shall give instructions about its safe keeping. This is a general provision and does not specify where the data must be stored specifically given that the Attorney General has competence to order such location.

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 may be stored outside Cyprus. The Data Protection Law provides that is a Service Provider is using the services of a third party to store the data (in Cyprus or abroad) there must be a written contract between the Service Provider and a data processor. Where the data will be stored abroad outside the European Union, the said Law contains specific provisions regarding the "Transmission of data to third countries" and requires the issuing of a prior license of the Data Protection Commissioner for this purpose. The Commissioner shall issue the license if she considers that the said country ensures an adequate level of protection.

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

a) no data are retained beyond what is permitted?

According to the Data Protection Law, section 4, in order for the processing of personal data to be considered lawful, the data controller must ensure that the personal data are:

(a) Processed fairly and lawfully;

(b) Collected for specified, explicit and legitimate purposes and are not further processed in a way incompatible with those purposes;

(c) Relevant, appropriate and not excessive in relation to the purposes of processing;

(d) Accurate and, where necessary, kept up to date;

(e) Kept in a form which permits identification of data subjects for no longer than is necessary, in the Commissioner's discretion, for the fulfilment of the purposes for which they were collected and processed. After the expiry of this period, the Commissioner may, by a reasoned decision, allow the preservation of personal data for historical, scientific or statistical purposes if he considers that the rights of the data subjects or third parties are not affected.

The data controller shall be responsible for the destruction of personal data which have been collected or which are further processed in contravention of the above requirements. If the Data Protection Commissioner ascertains, either on her own initiative or following a complaint, that a contravention of the above requirements has occurred, he shall order the interruption of the collection or processing and the destruction of the personal data already collected or processed.

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)?

According to the Data Retention law, a court order must be obtained before accessing the data; otherwise it shall be an offence to gain access to data and use of such data shall be prohibited.

The Protection of Privacy of Private Communication (Monitoring Communications) of 1996 makes reference to the monitoring/tapping of private communications by electronic, mechanical, electromagnetic, acoustic or other devices or equipment. State bodies may access data by using such equipment and methods of monitoring. If such monitoring is carried out without a valid Court order it will be illegal.

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

According to the Data Protection Law, section 4, in order for the processing of personal data to be considered lawful, the data controller must ensure that the personal data are collected for specified, explicit and legitimate purposes and are not further processed in a way incompatible with those purposes and that they are relevant, appropriate and not excessive in relation to the purposes of processing.

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.

The Data Protection Law, section 10, provides, with regards to the "confidentiality and security of processing" that a controller (in this case a Service Provider) must take the appropriate organizational and technical measures for the security of data and their protection against accidental or unlawful destruction, accidental loss, alteration, unauthorised dissemination or access and any other form of unlawful processing. Such measures shall ensure a level of security which is appropriate to the risks involved in the processing and the nature of the data processed.

The processing must be carried out only by persons acting under the authority of the controller or the processor and only upon instructions from the controller.

With regards to data access by third parties under authority of the data controller, if processing is performed by a data processor (e.g. a third party), the assignment for the processing must be made in writing. The assignment must provide that the processor shall perform the processing only upon instructions from the controller and that the above obligations shall also lie on the processor.

The Data retention Law provides that the disclosure of the content of any communication shall be prohibited (section 12). In addition, the said Law imposes an obligation for the protection and security of data and provides that for this purpose the relevant provisions of the Data Protection Law and the Electronic Communications Law shall apply (section 14(1)).

In addition and without prejudice to the above, Service Providers are subject to an obligation to (section 14(2)):

(a) Ensure that the retained data shall be of the same quality and subject to the same security and protection as those data on the network;

(b) Protect the retained data by taking appropriate technical and organisational measures against accidental or unlawful destruction, accidental loss or alteration, or unauthorised or unlawful storage, processing, access or disclosure;

(c) Ensure that only specially authorised personnel can have access to the retained data and keep a register of authorized personnel as well as a register where all access of authorized personnel to retained data shall be recorded, as well as the date and time and purpose of access;

The Data Retention Law also refers to the protection of privacy of personal communications (section 22 of the Data Retention Law) in accordance with the provisions of the Protection of Privacy of Personal Communications Law. Finally, it is a criminal offence for any person to gain access to retained data without a valid Court order or to disclose data which he became aware of to any third parties regarding the procedure for the investigation of a serious crime.

The Electronic Communications Law provides the following regarding security:

(a) ***Security of network and services***: In section 98 it is provided that public electronic communications network and/or services providers shall take all necessary technical and administrative measures in order to safeguard the security of their networks and services, at a level which is commensurate with the degree of risk having regard to the cost of implementation of such security systems and the latest technical possibilities. In case there is a particular risk of a breach of security of the network, the providers shall inform their subscribers of such risk and for all possibilities of avoidance, including the cost involved.

(b) ***Confidentiality and data protection:*** The providers referred to in Section 98, as well as their employees, shall take the appropriate technical and organisational measures to safeguard the security of their services and the confidentiality of any communication. No person, other than users communicating between themselves from time to time, shall be allowed to listen to, tap, store, intercept and/or undertake any other form of surveillance of communications without the consent of the users concerned, except to the extent that interceptions of communications occur in circumstances provided for by the law and with the authorisation of a court.

(c) The use of electronic communications networks to store information or to gain access to information stored in the terminal equipment of a subscriber or user is only allowed on the condition that the subscriber or user concerned is provided with clear and comprehensive information, inter alia about the purposes of the processing, and is offered the right to refuse such processing by the data controller. This shall not prevent any technical storage or access for the sole purpose of carrying out or facilitating the transmission of a communication over an electronic communications network, or as strictly necessary in order to provide an information society service explicitly requested by the subscriber or user.

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

According to section 14 of the Data Retention Law, a Service Provider has an obligation to destroy the data at the end of the period of retention, except those that have been ordered by the Court to be accessed and ordered to be preserved separately.

According to section 100 of the Electronic Communications Law, traffic data concerning subscribers and users, which are submitted to processing so as to establish communications and which are stored by service providers, shall be erased or made anonymous at the end of a call. The processing of the above data is permitted only up to the end of the period in which a bill may be lawfully challenged and/or payment pursued

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)?

The Data Protection Law, section 11, provides for the "Right of Information" of data subjects. More specifically, the data controller (in this case a Service Provider) shall, at the time of collection of the personal data from the data subject, provide the latter, in an appropriate and explicit way, with at least the following information:

(a) his identity and the identity of his representative, if any;

(b) the purpose of the processing;

The controller shall also inform the data subject about the following:-

(a) the recipients or the categories of recipients and of the data; and

(b) the existence of the right of access to and

Further to the above, according to section 99 of the Electronic Communications Law, the use of electronic communications networks to store information or to gain access to information stored in the terminal equipment of a subscriber or user is only allowed on the condition that the subscriber or user concerned is provided with clear and comprehensive information, inter alia about the purposes of the processing, and is offered the right to refuse such processing by the data controller. This shall not prevent any technical storage or access for the sole purpose of carrying out or facilitating the transmission of a communication over an electronic communications network, or as strictly necessary in order to provide an information society service explicitly requested by the subscriber or user.

According to section 101 of the Electronic Communications Law, where location data other than traffic data relating to users or subscribers of public communications networks or publicly available electronic communications services can be processed, such data may only be processed when they are made anonymous, or with the consent of the users or subscribers to the extent and for the duration necessary for the provision of a value added service. The service provider must inform the users or subscribers, prior to obtaining their consent, of the type of location data other than traffic data which will be processed, of the purposes and duration of the processing and whether the data will be transmitted to a third party for the purpose of providing the value added service. Users or

subscribers shall be given the possibility to withdraw their consent for the processing of location data other than traffic data at any time.

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

According to the Data Protection Law, section 6, the collection and processing of sensitive data is generally prohibited unless certain conditions are fulfilled as specifically prescribed by the Law. Sensitive data according to the Data Protection Law are data concerning racial or ethnic origin, political opinions, religious or philosophical beliefs, participation in a union, club or trade union organisation, health, sexual life and sexual orientation, as well as anything relevant to criminal prosecutions or sentencing. Said data may be ‚processed', a term which includes retention and transmission. .

Section 6 of the Law provides that the collection and processing of sensitive data is generally prohibited although it then sets out a number of exceptions to this general principle:

(1) The data subject has given his explicit consent. If the consent was extracted unlawfully or is contrary to morals, custom or a specific law, consent does not cancel the prohibition.

(2) The processing is necessary for the data controller to fulfil his obligations or to carry out his duties under employment law and the Commissioner has given a permit for this purpose.

(3) The processing is necessary for the preservation of a vital interest of the data subject or of another person, if the data subject is physically or legally unable to give his consent.

(4) The processing is carried out by an institution, club or any other non-profit making organisation which has political, philosophical, religious or trade union objects, and only concerns its members and any other persons with which the aforesaid club, institution or organisation keeps links due to its objects. These data can be disclosed to third parties only if the data subject consents.

(5) The processing concerns exclusively data which the data subject notifies to, or which are necessary for the ascertaining, exercise or defence of a right before, a court.

(6) The processing is necessary on the grounds of national interest or the needs of national security, or criminological or correctional policy needs, that is carried out by a service of the Republic or organisation or institution authorised for that purpose by a service of the Republic and concerns the investigation of crimes, criminal sentencing, security measures and investigation into major disasters (*e.g.* natural disasters or large scale destruction caused by terrorist or other criminal activity).

(7) The processing is carried out exclusively for statistical, research, scientific and historical purposes, provided that all the necessary measures for the protection of the data subjects are taken.

(8) The processing is carried out exclusively for journalistic purposes or within the framework of artistic expression and provided that the right to the protection of private and family life is not violated in any way.

The Law provides that the Council of Ministers can issue regulations providing for the processing of sensitive personal data in cases other than those mentioned above, when there are important reasons of public interest

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)?

Control that the aforementioned measures are effectively applied vest in the Data Protection Commissioner. According to the Data Protection Law, the Data Protection Commissioner has the following relevant competencies:

(a) To report any contraventions of the provisions of this Law to the competent authorities;

(b) To impose administrative sanctions;

(c) To assign to a member of her Office the conduct of administrative inquiries;

(d) To conduct, on her own initiative or following a complaint, an administrative inquiry on any filing system;

In addition, the Data Protection Commissioner has the following powers in its role as the Supervising Authority for the purpose of monitoring the application of the provisions of the Data Retention Law:

(a) Carry out examinations, to examine complaints and impose administrative fines by virtue of the Data Protection Law on data processors regarding violations of the Data Retention Law;

(b) In the event of possible prima facie violation consisting in a criminal offence by virtue of the provisions of the Data Retention Law, submit information which it has at its disposal before the Attorney General of the Republic who shall decide whether there is any criminal liability justifying criminal prosecution of the offender.

(c) Deal with the case herself and impose any sanctions foreseen by the Data Protection Law which are suitable in her opinion.

There is no other requirement for any other type of data protection audit, (in-house or public) data protection officer or external auditors.

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 Data Protection Law, section 10, provides, with regards to the "confidentiality and security of processing" that a controller (in this case a Service Provider) must take the appropriate organizational and technical measures for the security of data and their protection against accidental or unlawful destruction, accidental loss, alteration, unauthorised dissemination or access and any other form of unlawful processing. Such measures shall ensure a level of security which is appropriate to the risks involved in the processing and the nature of the data processed.

The said Law also provides that the Data Protection Commissioner shall give, from time to time, directions with regard to the degree of security of the data and to the measures of protection required to be taken for every category of data, taking also into account technological developments. No such directions have been taken by the Data Protection Commissioner at the time of writing.

The Electronic Communications Law provides the following regarding security:

- ***Security of network and services:***

  In section 98 it is provided that public electronic communications network and/or services providers shall take all necessary technical and administrative measures in order to safeguard the security of their networks and services, at a level which is commensurate with the degree of risk having regard to the cost of implementation of such security systems and the ***latest technical possibilities***. In case there is a particular risk of a breach of security of the network, the providers shall inform their subscribers of such risk and for all possibilities of avoidance, including the cost involved.

- ***Confidentiality and data protection:***

  The providers referred to in Section 98, as well as their employees, shall take the appropriate technical and organisational measures to safeguard the security of their services and the confidentiality of any communication. No person, other than users communicating between themselves from time to time, shall be allowed to listen to, tap, store, intercept and/or undertake any other form of surveillance of communications without the consent of the users concerned, except to the extent that interceptions of communications occur in circumstances provided for by the law and with the authorisation of a court.

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.

The Data Retention Law does not contain any specific technical rules regarding the cooperation between the Police Investigator and the Service Provider retaining the data, other than those rules set out in the reply to question 29 above.

Procedure-wise, according to section 5 of the Data Retention Law, where a Service Provider is presented with a data access order issued by the Court has an obligation to make available immediately and in any event without undue delay all data prescribed in the relevant Court order to the Police investigator

With regards to the cooperation between public authorities themselves, the said Law contains a rule that the Police Investigator needs to file an application to the Attorney General in order for the latter to approve the application for the issuing of a Court order.

The Attorney General needs to be satisfied that the issuing of the Court order is capable of providing evidence regarding the commission of the serious criminal offence. The aforementioned application to the Attorney General must be made in writing and must have as attachment an affidavit of the Police Investigator containing certain information enumerated in section 4 of the Law. After approval of the application by the Attorney General, an application is filed before the competent Court for the issuing of a court order authorizing access to the data.

No regulations or orders have been issued establishing such technical or organisational rules.

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?

- ***Mutual Assistance in Criminal Matters between the Member States of the European Union***

  By virtue of the Law N. 25(III)/2004 ratifying the Convention established by the Council in accordance with Article 34 of the Treaty on European Union, on Mutual Assistance in Criminal Matters between the Member States of the European Union (OJ C 197, 12.7.2000, p. 3) as well as its Protocol, the requested Member State shall execute the request for assistance as soon as possible, taking as full account as possible of the procedural deadlines and other deadlines indicated by the requesting Member State.

  Each Member State shall send procedural documents intended for persons who are in the territory of another Member State to them directly by post, subject to certain exceptions (Article 4 of the Convention).

Requests for mutual assistance and spontaneous exchanges of information referred to in Article 7 shall be made in writing, or by any means capable of producing a written record under conditions allowing the receiving Member State to establish authenticity. Such requests shall be made directly between judicial authorities with territorial competence for initiating and executing them, and shall be returned through the same channels unless otherwise specified.

Where there is reason to believe that the addressee does not understand the language in which the document is drawn up, the document, or at least the important passages thereof, must be translated into (one of) the language(s) of the Member State in the territory of which the addressee is staying (Article 5 of the Convention).

- ***Mutual Legal Assistance between the United States of America and Cyprus***

The Republic of Cyprus has ratified the Instrument (the "Instrument") as contemplated by Article 3(2) of the Agreement on Mutual Legal Assistance between the United States of America and the European Union signed on 25 June 2003, as to the application of the Treaty (the "Treaty") between the Government of the United States of America and the Government of the Republic of Cyprus on Mutual Legal Assistance in Criminal Matters signed 20 December 1999.

Cross border requests for legal assistance are transmitted between the Central Authorities. Requests for assistance must be made in writing (e.g. by fax or email) unless urgent. Requests need to contain certain information, including, inter alia, the name of the authority conducting the investigation, a description of the subject matter and nature of the investigation, a description of the evidence, information or other assistance sought and a statement of the purpose for which assistance is sought. The Central Authority of the requested State shall execute promptly the request or transmit it to the authority having jurisdiction to do so. The competent judicial or other authorities of the requested State shall have power to issue subpoenas, search warrants or other orders necessary to execute the request.

The application for legal assistance is filed in the language of the requesting party, together with a translation in the language of the recipient country unless agreed otherwise.

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).

- ***Data Protection Officers:***

  The Office of the Data Protection Commissioner did not take an active role concerning the retention of data and its implementation. The only known activity undertaken is its participation in some Conferences of European Data Protection Authorities, the works of the Article 29 Working Party and in the joint adoption of declarations or common positions on the matter.

  In this respect, the Data Protection Commissioner participated in the adoption of the "Common position of the European Data Protection Authorities on the use of the concept of availability in law enforcement", adopted on 11 May 2007.

- ***Businesses – Service Providers:***

  There has been extensive discussion before the House of Representatives involving ISPs in the discussion prior to the adoption of the Data Retention Law. The ISPs did not regard the introduction of the Law as a positive step due to the high costs involved for them for the retention of data for such a long period of time. They considered that the retention of data would be increasing their costs and lowering their profitability. In addition, before the enactment of the Law, on certain occasions the Cyprus Police has requested certain ISPs to disclose data available to them in order to facilitate the investigation of serious crimes (such as child pornography). One ISP so requested refused to disclose the location data of one of its customers even though that would have led to the arrest of the said client. Even after the adoption of the Law the same ISP refused to disclose the relevant data until a Court order was issued.

  The Cyprus Police is known to have used the provisions of the Data Retention Law in order to access data for the purpose of investigating crimes. It sees the adoption of the Law as a positive step in facilitating its work.

  No other reports have been made on the matter and no measures are known to have been taken in Cyprus from political parties, civil rights groups, labour unions, etc.

  It should however been noted that following a long discussion on the matter of privacy and access to private communications, the House of Representatives has adopted Law 51(I) of 2010, amending Article 17 of the Constitution on the 4th of June 2010 (the Sixth Constitutional Amendment Law) which provides that the Attorney General can authorize phone tapping. The amendment also allows the police to monitor web logs, downloads and emails as admissible evidence for criminal investigations.

It may be presumed that any type of data may be retained including traffic data. The Constitution does not refer to an exclusion of traffic data. It will depend on the case under consideration.

Article 17 currently provides that (1) "Every person has the right to respect for, and to the secrecy of, his correspondence and other communication if such other communication is made through means not prohibited by law"; and (2) "There shall be no interference with the exercise of this right except in the following cases: (a) convicted and non-convicted prisoners; (b) following a court order issued in accordance with the provisions of the law following an application by the Attorney General of the Republic and the intervention consists in a measure which in a democratic society is necessary solely for the interests of the security of the Republic or for the prevention, investigation or sanctioning of certain serious crimes (such as murder, child pornography, trading in drugs, etc); and (c) following a court order issued for the purposes of investigation of serious crimes sanctioned by imprisonment for a term exceeding 5 years and provided that the intervention concerns access to electronic communications traffic and location data and relevant data which is necessary for identifying the subscriber and/or user.

The aforementioned amending Law provides that the said amendment was enacted because according to the case law of the Supreme Court no person has the right unless authorized by the law for reasons prescribed by the Constitution, to monitor or interfere with the communications between citizens. In addition, the amendment was necessary in order to make possible the intervention where this is necessary for the purpose of securing the safety of the Republic as well as to prevent, investigate or sanction serious criminal offences.

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)?

As mentioned above, personal data must be processed for a specific purpose only.

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.

A report was prepared by a private company Cryptohippie entitled Electronic Police State Data 2009. The results are available on https://secure.cryptohippie.com/

The following results were reported:

Daily Documents	Border Issues	Financial Tracking	Gag Orders	Anti-Crypto Laws
2	2	3	3	2

Constitutional Protection	Data Storage Ability	Data Search Ability	ISP Data Retention	Telephone Data Retention
2	2	1	2	2

Cell Phone Records	Medical records	Enforcement Ability	Habeas Corpus	Police-Intel Barrier
2	1	3	3	3

Covert Hacking	Loose Warrants	Total	Ranking
2	2	3	2.17647059

According to a relevant article published in the Cyprus Mail, a local newspaper, (By Elias Hazou Published on May 14, 2009):

"CYPRUS has been placed 37th in the 2008 national rankings for the 'Electronic Police State' compiled by Cryptohippie Inc., a consortium of US providers of 'privacy enhancing technologies'.

Cryptohippie clarifies that its rankings, released every year, do not measure government censorship of Internet traffic or police abuses, "as legitimate as these issues may be."

Out of a maximum score of 5 (1 being the least sinister of government and police surveillance), the Mediterranean island scored 2.176."

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?

No such information has been located.

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?

There was some discussion especially in the newspapers and the media at large concerning the retention of data from public cameras installed in roads for the purpose of traffic offences.

In addition, as mentioned above, following a long discussion on the matter of privacy and access to private communications, the House of Representatives has adopted Law 51(I) of 2010, amending Article 17 of the Constitution on the 4th of June 2010 (the Sixth Constitutional Amendment Law) which provides that the Attorney General can authorize phone tapping. The amendment also allows the police to monitor web logs, downloads and emails as admissible evidence for criminal investigations.

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) law1 – 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 Cyprus establishes in its Chapter II several fundamental rights and freedoms.[2] Article 34 of the Constitution binds every branch of the Cyprus State including the Judiciary to safeguard the efficient application of the rights entrenched in that part of the Constitution.

The Right of Privacy is safeguarded by Article 15.1 of the Constitution that reads:

"1. Every person has the right to respect for his private and family life.

2. There shall be no interference with the exercise of this right except such as is in accordance with the law and is necessary only in the interests of the security of the Republic or the constitutional order or the public safety or the public order or the public health or the public morals or for the protection of the rights and liberties guaranteed by this Constitution to any person."

---

1 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).

2 Chapter II of the Constitution, without its amendments, can be found through this link http://www.kypros.org/Constitution/English/appendix_d_part_ii.html

Article 15.1 is modelled on Article 8 of the European Convention of Human Rights that proclaims a right to privacy as such; in turn fashioned in the spirit of the 1948 U.N. Universal Declaration of Human Rights.

The right to secrecy of correspondence is safeguarded by Article 17 of the Constitution. Article 17 was amended on the 4th of June 2010 by Law 51(I) of 2010 (the "Sixth Amendment of the Constitution") and currently provides that:

(1) "Every person has the right to respect for, and to the secrecy of, his correspondence and other communication if such other communication is made through means not prohibited by law"; and

(2) "There shall be no interference with the exercise of this right except in the following cases: (a) convicted and non-convicted prisoners; (b) following a court order issued in accordance with the provisions of the law following an application by the Attorney General of the Republic and the intervention consists in a measure which in a democratic society is necessary solely for the interests of the security of the Republic or for the prevention, investigation or sanctioning of certain serious crimes (such as murder, child pornography, trading in drugs, etc); and (c) following a court order issued for the purposes of investigation of serious crimes sanctioned by imprisonment for a term exceeding 5 years and provided that the intervention concerns access to electronic communications traffic and location data and relevant data which is necessary for identifying the subscriber and/or user.

The aforementioned amending Law provides that the said amendment was enacted because according to the case law of the Supreme Court no person has the right unless authorized by the law for reasons prescribed by the Constitution, to monitor or interfere with the communications between citizens. In addition, the amendment was necessary in order to make possible the intervention where this is necessary for the purpose of securing the safety of the Republic as well as to prevent, investigate or sanction serious criminal offences.

The right conferred by Article 17 is, on the face of its wording, far reaching and extends prima facie to every written and oral communication, provided always it is carried out by means not prohibited by law. "Communication" signifies imparting something orally or in writing (correspondence), with a view to bringing it to the notice of another or others, in the context of an exchange of views, feeling or ideas. Like privacy, it aims to secure maximum freedom for the individual in his private exchanges.

The notion of "correspondence" includes not only letters in paper form but also other forms of electronic communications received at or originated from the workplace, such as telephone calls made from or received at business premises or e-mails received at or sent from the offices' computers.

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 Right of Privacy safeguarded by Article 15.1 of the Constitution may be limited if this is necessary only in the interests of the security of the Republic or the constitutional order or the public safety or the public order or the public health or the public morals or for the protection of the rights and liberties guaranteed by this Constitution to any person.

The right to secrecy of correspondence which is safeguarded by Article 17 of the Constitution may be interfered with in the following cases:

(a) communication of convicted and non-convicted prisoners;

(b) following a court order issued in accordance with the provisions of the law following an application by the Attorney General of the Republic and the intervention consists in a measure which in a democratic society is necessary solely for the interests of the security of the Republic or for the prevention, investigation or sanctioning of certain serious crimes (such as murder, child pornography, trading in drugs, etc); and

(c) following a court order issued for the purposes of investigation of serious crimes sanctioned by imprisonment for a term exceeding 5 years and provided that the intervention concerns access to electronic communications traffic and location data and relevant data which is necessary for identifying the subscriber and/or user.

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?

Only one civil case has been located regarding the issuing of an Order of Certiorari dated 21/01/2010, Case No 1/2010. The case title is as follows:

"Application of Andreas Alexandrou for permission of the Supreme Court to file an application for the Issuing of an Order of Certiorary by virtue of Article 155 of the Constitution and sections 3 and 9 of the Award of Justice (Miscellaneous Provisions) Law of 1964 and Articles 1A, 15, 17 and 30 of the Constitution, Law 183(I)/2007 and Directive 2006/24/EC and with respect to the Order for the Disclosure of Telecommunications Data issued by the District Court of Nicosia on 5/8/2009."

The case is not subject to appeal because the decision was adopted by the Supreme Court (the highest court of the Republic) and has not been appealed.

The case concerned the claim that the Court Order was issued in excess of jurisdiction in view of the fact that the provisions of the Data Retention Law were not covered by the provisions of Article 1A of the Constitution because the Law was erroneously adopted for the purpose of preservation of telecommunications data for the purpose of investigation of criminal offences and was thus contrary to the provisions of Directive 2006/24/EC by virtue of which the data Retention Law had

been adopted. The lawyer of the applicant referred to the scope/purpose of the Directive as set out in the decision of the European Court of Justice in the case Ireland v. European Parliament and Council of the European Union, Case no. C301/06 dated 10.2.09, which explained the scope/purpose of the Directive.

The Supreme Court decided that the lifting of the confidentiality of telecommunications data was contrary to fundamental right established by Article 17 of the Constitution (Right of Privacy of Communications). The violation of constitutional provisions consists in excess of competence and a Court decision issued in excess of competence lacks competence. The Supreme Court also decided that the Retention of Data Law does not contain any provisions for the right to appeal and as a result, on the basis of established case law, this provided a right for the filing of an application for the issuing of an order of certiorari in order to examine the compatibility of the order issued by the Court of First Instance with Articles 15 and 17 of the Constitution.

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?

The limit is not absolute but an assessment/balance of interests to be carried out in each individual 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)?

There are no other exemptions except as those referred to above.

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?

According to Cypriot jurisprudence, the right to privacy extends to inherently private, personal and family matters objectively identifiable as such. This is always on condition that the beneficiary of the right has not by his own action exposed the matter to public view.

As a result, trading and business activities are not of their nature private personal matters since they involve impersonal conduct with the public. For example, the relationship between trader and customer is commercial and not confidential and a

trader's transactions with different customers do not make the relationship confidential.

In the case of *CHARALAMBOS TILEMACHOU PSARAS*, v. *THE REPUBLIC*,[3] the content of a telephone directory kept by an employee was not found, of itself, to be a document embodying inherently personal records in the sense of Article 15.1. If the employee leaves the directory exposed on his desk and within reach of other personnel of the company, he can have no expectation that its content and matters included therein should be kept private to him. The claim to privacy in relation to the directory collapsed altogether upon reflection that it was no part of the directory and that it was merely kept or stored therein

Where Article 17 of the Constitution is concerned, according to the case law, the rapid development of technology in recent years has created vast dangers for human rights. The right to privacy is at risk from a wide variety of devices, such as electronic acoustics, recordings of conversation - optical, film and photographic - and the computerisation and assembly of data by individuals, the State, private institutions and organisations. The right to privacy may be imperilled by the use of anyone or more of the aforementioned devices, whether used by the State or anybody else. Therefore, for the protection to be effective, it must extend against everyone.

In the case of *The Police* v. *Andreas Georghiades*[4] it was held that "…the scope of the protection of privacy under [Article 8] of the Convention remains largely unexplored in the case-law. It has been suggested that the Convention protects the individual, under this heard, against, *inter alia*, the use of his name, identity, or likeness, being spied upon, watched, or harassed, and the disclosure of information protected by the duty of professional secrecy…"

In the case of *Police* v. *Christodoulou Yiallourou*[5], the Court held that a telephone conversation, due to its nature, is objectively an aspect of private life on the basis of Article 15.1 and a form of communication safeguarded by Article 17.1. No third person has the right, unless authorized by Law, to spy on telephone conversations of other citizens.

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)?

According to the Data Retention Law, private companies (Service Providers) are called upon to grant access to data retained on the basis of an order issued by the Court in order to enable a police investigator to obtain evidence that a serious criminal offence has been committed.

---

3 (1987) 2 C.L.R. 132.

4 (1983) 2 C.L.R. 33.

5 (1992) 2 C.L.R. 147.

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

There is no such requirement.

III. Dimension 3 (State – State)

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

According to Article 169(3) of the Constitution of the Republic of Cyprus, treaties, conventions and agreements concluded shall have, as from their publication in the official Gazette of the Republic, superior force to any municipal law on condition that such treaties, conventions and agreements are applied by the other party thereto.

The European Convention on Human Rights and Fundamental Freedoms of 1962, which was signed by the Republic on November 24, 1961, was ratified on May 24, 1962. By the ratification, the general right to privacy under Section 8 of the Convention is effectively guaranteed.

Law No. 28(III)/2001 also ratified the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data of 1981. The Convention was signed by the Republic of Cyprus on July 25, 1986 and ratified on November 23, 2001 (on the same day as the date of entry into force of the Data Protection Law). The Ratifying Law appoints the Data Protection Commissioner as the competent authority in the Republic of Cyprus for exercising all of the powers and competence provided by the Convention.

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?

Pursuant to the Treaty of Accession signed in Athens on 16 April 2003 and ratified with the Treaty of Accession of the Republic of Cyprus to the European Union (Ratification) Law, 2003, the Republic acceded to the European Union on 1 May 2004. The Republic of Cyprus is bound and obliged to apply the provisions of the Treaties establishing the European Communities and the Treaty on European Union and the acts of the institutions of the European Communities and the European Union.

In order for the Republic as a Member State of the European Union to be in a position to exercise every option and discretionary power conferred upon it by the European Communities and the European Union Law it enacted the Fifth Amendment of the Constitution Law, 2006.

In its Preamble, the Law states the following:

- There are provisions of the Constitution which are incompatible with the ability of the Republic to comply with the aforementioned commitments and obligations and put obstacles in the capability of the Republic to exercise its options and discretionary power conferred upon it as a Member State of the European Union,

- By the addition of a new article and the amendment of Articles 140, 169 and 179 of the Constitution, which are not included in the basic articles, the aforesaid incompatibility and obstacles may be removed,

- Owing to the development in the field of international judicial cooperation in criminal matters, the Republic has undertaken a conventional obligation to extradite or surrender its own citizens/nationals committing criminal offences in a foreign country,

- The addition of a new article and the amendment of the aforementioned provisions of the Constitution are absolutely necessary for achieving the goal of creating the legal conditions, which will allow the Republic to function under normal conditions as a Member State of the European Union, exercising all the rights and complying with all obligations of such Member State.

As a result, the Constitution was amended by the addition, immediately of the following new Article 1A:

"Article 1A.

No provision of the Constitution shall be deemed to have annulled laws enacted, acts done or measures taken by the Republic that are deemed necessary due to its obligations as a Member State of the European Union, neither does it prevent Regulations, Directives or other Acts or binding measures of a legislative character, adopted by the European Union or the European Communities or by their institutions or competent bodies thereof on the basis of the Treaties establishing the European Communities or the Treaty on European Union, from having legal effect in the Republic."

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?

As analysed below, the Cyprus constitutional law does not limit the possibility of transferring national sovereignties to the European Union.

Article 1 of the Constitution provides that the State of Cyprus is an independent and sovereign Republic. Certain international treaties become applicable in Cyprus if ratified by an Act of Parliament and published in the Official Gazette. Under Article 169 (3) they prevail over 'municipal law'. In the Republic of Cyprus, the rigid Constitution of 1960 is the supreme law of the land, as expressly stated in Article 179. Cypriot jurisprudence specifies that this principle does not touch upon the supremacy of the Constitution laid down in Article 179 (1) of the Constitution. Rather, the term 'municipal law' in Article 169 (3) refers to ordinary statutes and regulations. Hence, ratified international treaties enjoy a rank over other statutes, but below the Constitution.

For the purpose of accommodating the Principle of Supremacy of Community Law to the Cypriot Legal Order a Constitutional Amendment was deemed necessary as described in the answer in question 59.[6]

The special constitutional significance of EU membership was recognised shortly after accession by the passage of specific EU integration clauses.

Several Articles on the powers of State institutions were identified as being potentially incompatible with EU membership. Following this analysis, a modification of the Constitution prior to EU accession was deemed necessary.

Under Section 4, the Treaty of Accession only supersedes other legislative or regulatory acts. The shortcomings of this approach, however, soon became apparent in a case involving a Cypriot citizen whose transfer to the UK was demanded by British authorities according to the European Arrest Warrant. As Article 11 of the Cypriot Constitution contained a provision according to which Cypriot citizens cannot be extradited, the Supreme Court of Cyprus confirmed the non-extradition of the person. That decision was in conformity with Cypriot law, but in defiance of EU law. Thereafter, on 28 July 2006, the House of Representatives passed a constitutional amendment. Under the new Article 1A of the Cyprus Constitution, none of its provisions prevent Regulations, Directives or other acts or binding measures of a legislative nature enacted by the European Union or by the European Communities or by their institutions or bodies from having legal force in the Republic.

---

6 **Constitutional Implications of EU Membership: A View from the Commission,** Frank Hoffmeister, Published in Croatian Yearbook of European Law and Policy, Vol. 3 (2007), pp. 59-97.

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?

Data retention related powers have been vested to the Cyprus Police (under the Ministry of justice and Home Affairs) and the Attorney General (an independent officer of the Republic in accordance with the Constitution). The Data Protection Commissioner is also an independent organ of the State.

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

The transmission of retained data must be made in accordance with the provisions of the Data Protection Law (regarding transmission by ISPs themselves) or, where the transmission is carried out by national competent authorities, this must be done in accordance with the provisions of the Treaties ratified by the Republic which according to Article 169(3) of the Constitution of the Republic of Cyprus, gain, as from their publication in the official Gazette of the Republic, superior force to any municipal law on condition that such treaties, conventions and agreements are applied by the other party thereto.

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 Data Retention Law should perhaps be amended in order to contain provisions for the right to appeal against a court order. The Law should also include rules governing the manner in which and location where the retained data shall be kept after they have been accesses to by Police Investigators. At the moment, the Law is silent and does not contain any specific rules on this manner and only contains a general provision that the data accessed shall be kept secure after their access.

In addition, due to the large costs involved in the retention of data by ISPs, perhaps an improvement would be to reimburse such ISPs in order to safeguard consumers from incurring the increase of rates as a result of high retention costs. Retention costs could also be reduced if the nature or categories of the retained data is limited.

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

Cyprus

Olga Georgiades

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 Cyprus establishes in its Chapter II several fundamental rights and freedoms.[1] The Right of Privacy is safeguarded by Article 15.1 of the Constitution that reads:

"1. Every person has the right to respect for his private and family life.

2. There shall be no interference with the exercise of this right except such as is in accordance with the law and is necessary only in the interests of the security of the Republic or the constitutional order or the public safety or the public order or the public health or the public morals or for the protection of the rights and liberties guaranteed by this Constitution to any person."

Article 15.1 is modelled on Article 8 of the European Convention of Human Rights that proclaims a right to privacy as such; in turn fashioned in the spirit of the 1948 U.N. Universal Declaration of Human Rights.

According to Cypriot jurisprudence, the right to privacy extends to inherently private, personal and family matters objectively identifiable as such. This is always on condition that the beneficiary of the right has not by his own action exposed the matter to public view.

As a result, trading and business activities are not of their nature private personal matters since they involve impersonal conduct with the public. For example, the relationship between trader and customer is commercial and not confidential and a

[1] Chapter II of the Constitution, without its amendments, can be found through this link http://www.kypros.org/Constitution/English/appendix_d_part_ii.html

trader's transactions with different customers do not make the relationship confidential.

The right to secrecy of correspondence is safeguarded by Article 17 of the Constitution Article 17 was amended on the 4th of June 2010 by Law 51(I) of 2010 (the "Sixth Amendment of the Constitution") and currently provides that (1) "Every person has the right to respect for, and to the secrecy of, his correspondence and other communication if such other communication is made through means not prohibited by law"; and (2) "There shall be no interference with the exercise of this right except in the following cases: (a) convicted and non-convicted prisoners; (b) following a court order issued in accordance with the provisions of the law following an application by the Attorney General of the Republic and the intervention consists in a measure which in a democratic society is necessary solely for the interests of the security of the Republic or for the prevention, investigation or sanctioning of certain serious crimes (such as murder, child pornography, trading in drugs, etc); and (c) following a court order issued for the purposes of investigation of serious crimes sanctioned by imprisonment for a term exceeding 5 years and provided that the intervention concerns access to electronic communications traffic and location data and relevant data which is necessary for identifying the subscriber and/or user.

The aforementioned amending Law provides that the said amendment was enacted because according to the case law of the Supreme Court no person has the right unless authorized by the law for reasons prescribed by the Constitution, to monitor or interfere with the communications between citizens. In addition, the amendment was necessary in order to make possible the intervention where this is necessary for the purpose of securing the safety of the Republic as well as to prevent, investigate or sanction serious criminal offences.

The right conferred by Article 17 is, on the face of its wording, far reaching and extends prima facie to every written and oral communication, provided always it is carried out by means not prohibited by law. "Communication" signifies imparting something orally or in writing (correspondence), with a view to bringing it to the notice of another or others, in the context of an exchange of views, feeling or ideas. Like privacy, it aims to secure maximum freedom for the individual in his private exchanges.

The notion of "*correspondence*" includes not only letters in paper form but also other forms of electronic communications received at or originated from the workplace, such as telephone calls made from or received at business premises or e-mails received at or sent from the offices' computers.

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?

No amendments have been made to the current data retention legislation. It should be noted that the Cyprus Supreme Court decided on 1 February 2011 that some of the provisions of Law 183 (I) / 2007 on disclosure of telecommunications data are unlawful, as they breach the Cyprus Constitution and its jurisprudence.

In the case brought to the Supreme Court, four people claimed that Articles 4 and 5 of the national law, that provided police forces access to the retained data, were unlawful. The court considered that the articles in question go beyond the provisions of the EU Directive which does not address the issue of access to the retained data. Therefore, the court considered it may check the constitutionality of these articles, especially in relation with Art 15 of the Cyprus Constitution (right to privacy) and article 17 (confidentiality of communications).

Based on the Cyprus Constitution, and jurisprudence from itself and from the EctHR, the Supreme Court issued a unanimous ruling regarding the legality of court orders issued for the disclosure of telecommunications data by the district courts of Nicosia, Limassol and Larnaca at the request of police investigating serious crimes. The orders concerned the four complainants that claimed a breach of privacy and confidentiality of their communications.

The court considered that three of the four court orders for disclosing telephone numbers and calls were illegal and should be annulled. In the case of the fourth person the case was rejected, since the person was imprisoned and banned for using a mobile phone.

However, this does not mean that the legislation is bound to be amended in order to reflect the decision of the Supreme Court. It is unclear how this decision will affect the law and its application.

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?**

There are various instances where the law obligates citizens and undertakings to retain data and to co-operate with public authorities. Some examples are provided below.

<u>The Protection of Competition Law of 2008</u>

The Commission for the Protection of Competition is afforded the power to collect information and to carry out inspections.

«30.–(1) The Commission may collect information that is necessary for the exercise of its functions, powers and duties under this Law, both on its behalf as well as on behalf of other Competition Authorities, by addressing to that effect a written request to undertakings, associations of undertakings or other natural or legal persons...»

« (3) The person, or the association of undertakings or the undertaking to whom the request by the Commission is addressed to, shall be bound to provide in due course, in full and accurately the required information within the time-limit fixed...»

«31. –(1) The Commission may, in the exercise of its functions, powers and duties under this Law, conduct all necessary inspections of undertakings or associations of undertakings and for this purpose –

(a) Enter any office, premises, land and means of transport of undertakings and associations of undertakings, with the exemption of residences;

(b) Examine the records, books, accounts, and other records related to the business, irrespective of the medium on which they are stored;

(c) copy and photocopy records, books, accounts and other records related to the business, irrespective of the medium on which they are stored, and receive copies and photocopies;

(d) Seal any business premises and records, books, accounts and other business records, for the period and to the extent necessary for the inspection;

(e) Ask any representative or member of staff of the undertaking or association of undertakings, for explanations on facts or documents relating to the subject-matter and purpose of the inspection and record the answers....»

Central Bank of Cyprus Laws of 2002-2007

Obligation to report data to the Bank.

«63. Without prejudice to the obligation to report statistical information to the European Central Bank according to Article 5 of the Statute and the complementary European Union Legislation adopted in accordance with the said Article, banks, government services, public corporations, as well as any natural person or legal entity shall be required, without being entitled to invoke bank or other secrecy, to report to the Bank all the data and information in their possession which are necessary for the fulfilment of its objectives as laid down in section 5 and for the performance of its tasks in accordance with section 6.»

Obligation to report data for the compilation of the balance of payments.

«64. (1) (a) The Bank may require from the natural persons and legal entities referred to in section 63 to report to the Bank all the data and information in their possession, which shall be specified in directives, issued by the Bank under

subsection (2), for the compilation of the balance of payments and the international investment position of the Republic as well as the financial accounts of the individual sectors of the economy.

(b) Natural persons and legal entities referred to in section 63 shall be required, without being entitled to invoke bank or other secrecy, to report to the Bank the data and information referred to in paragraph (a).

(2) The Bank may specify, by issuing pertinent directives, the data and information which the natural persons and legal entities referred to in section 63 are required to obtain and report in relation to their transactions and to their asset and liability position vis-à-vis residents or non-residents of Cyprus. The Bank may also determine the manner, time, procedure and every other relevant detail according to which these data and information are to be reported:

Provided that, the data and information shall be complete and reported to the Bank exactly as they were supplied to the aforementioned natural persons and legal entities.

(3) In order to meet the reporting requirement of data specified in directives issued by the Bank, banks and designated financial institutions carrying out transactions on behalf of residents with non-residents of Cyprus, shall be required to collect from the resident counterparties to such transactions these data or information.

(4) Notwithstanding anything in any Law in force for the time being, data or information reported to the Bank for the purposes of this section shall be covered by professional secrecy and it shall be prohibited to be disclosed to any natural person or legal entity or to any public authority, either by a person acting or having previously acted on behalf of the Bank, or by a person which acquires knowledge of these data or information:

Provided that, this prohibition shall not apply to the disclosure, in aggregate form, of the abovementioned data and information, provided that the identity of the persons or entities to which such data and information refer is not revealed.

(5) For the purposes of this section, the Bank may define the concept of "resident of Cyprus" by issuing pertinent directives.

(6) (a) Any person who contravenes any of the provisions of this section shall be guilty of an offence and in case of conviction, he shall be punished by a fine not exceeding 85.430,00 euro and, in case of a continuing offence, by a further fine of 1.708,00 euro for each day during which the offence shall continue.

(b) A Court hearing an offence of contravention of the provisions of this section, may in case of conviction, in addition to any penalty imposed to the convicted person by virtue of paragraph (a), order the immediate reporting to the Bank of the data or information which the Bank asked. »

Imposition of administrative fine.

«64A. In the event that the Bank in exercising its task to collect data and information shall find out an infringement of the obligation for reporting data and information under this Part, and to the extent that there is no provision for the exclusive competence of the European Central Bank to impose sanctions, the Governor may, after having heard the person concerned, impose an administrative fine not exceeding 102.516,09 euro and, in case of a continuing infringement, impose, in addition, an administrative fine not exceeding 854 euro for everyday during which the infringement shall continue.»

Prevention and Suppression of Money Laundering Activities Law of 2007 and 2010

Order for disclosure.

«45.-(1) Without prejudice to the provisions of other laws, in relation to the receipt of information or documents in the course of investigating the possible commission of offences, for the purposes of inquiry in relation to prescribed offences or in relation to inquiry for the determination of proceeds or instrumentalities, the court may, on the application of the investigator of the case, make an order for disclosure under the provisions of this Part.

(2) For the purposes of this section, inquiry shall also include an inquiry conducted abroad and investigator of the case in respect of investigation conducted abroad shall include any investigator under the provisions of any relevant law of the Republic who cooperates with the investigator of the case.

(3) Any person to whom an order of disclosure is addressed under section 46 (Conditions for the making of an order for disclosure), shall have an obligation to notify forthwith the investigator about any subsequent change in the information that has already been given under this section.

Conditions for the making of an order for disclosure.

46.-(1) The court before which an application for the making of an order for disclosure is submitted, may, if satisfied that the conditions of subsection (2) are fulfilled, make an order called order for disclosure, addressed to the person who appears to the court to be in possession of the information to which the application relates, calling upon the said person to disclose or produce the said information to the investigator or any other person specified in the order within seven days or within such a longer or shorter period of time as the court may specify in the order if it considers expedient under the circumstances.

(2) The conditions referred to in subsection (1) are that:

(a) there is a reasonable ground for suspecting that a specified person has committed or has benefited from the commission of a prescribed offence;

(b) there is reasonable ground for suspecting that the information to which the application relates is likely to be, whether by itself or together with other

information, of substantial value to the investigations for the purposes of which the application for disclosure has been submitted;

(c) the information does not fall within the category of privileged information;

(d) there is a reasonable ground for believing that it is in the public interest that the information should be produced or disclosed, having regard to:

(i) the benefit likely to result for the investigation from the disclosure or provision of the said information; and

(ii) the circumstances under which the person in possession of the information holds it.

(3) The order for disclosure-

(a) may also be made in relation to information which is in the possession of a government officer;

(b) shall have effect despite any obligation for secrecy or other restriction upon the disclosure of information imposed by law or otherwise;

(c) shall not confer any right for production or disclosure of information which is privileged.

(d) It is served only to the person who has in his possession the information referred to in the application.

Information contained in a computer.

47. Where the required information is contained in a computer-

(a) if the order directs the disclosure of such information, the order shall be enforced by the disclosure of this information in a visible and legible form;

(b) if the order directs the handing over of the information to the investigator or other person, the order shall be enforced by the handing over of the information to the investigator in a form which is visible, legible and portable.

Offences in relation to the disclosure of information.

48. Any person who discloses that, information or other relevant material regarding knowledge or suspicion for money laundering have been submitted to the Unit or makes a disclosure which may impede or prejudice the interrogation and investigation carried out in respect of prescribed offences or the ascertainment of proceeds, knowing or suspecting that the said interrogation and investigation are taking place, shall be guilty of an offence punishable by imprisonment not exceeding five years;

It is provided that, in case where a person exercising the professional activity of auditor or external accountant or legal professional, attempts to prevent a customer from getting involved in illegal activity, this shall not constitute a disclosure of information in the meaning ascribed to this section.»

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 evidence in court?**

Privilege

Privilege between client and lawyer

Client–lawyer communications exchanged at the time of providing legal advice are deemed to be confidential. The client cannot be forced to disclose what has been exchanged with his lawyer or to present any document of any kind that has been exchanged between him and his lawyer. As for the lawyer, he must obtain his client's permission prior to disclosing any document or communication. For the client to be able to use this privilege, he must first establish a client–lawyer relationship.

Where such a relationship is effectively created, it remains confidential after the termination of the relationship if the client so requests. In the case of *Republic v Alan Carl Ford62*—a criminal case—the defendant claimed that the confidentiality of his communications with his lawyer had been breached due to the fact that prison guards obtained the notes that had been prepared for his case. The defendant claimed that this violated his fundamental rights protected by Article 30.3 of the Constitution (which is equivalent to Article 6.3 of the Convention for the Protection of Human Rights and Fundamental Freedoms) concerning the right to a fair trial. The court held that there can be no violation of confidentiality of communication between client and lawyer, as this violates that party's rights of representation by a lawyer of his choice. As a result, any document or evidence that is the result of such a violation is precluded during trial.

Where communications between a client or his lawyer and third parties are concerned, they are also deemed to be confidential but also when the case is still pending or is about to commence. If the client does not intend to file an action before the courts, then any document created by a third party (such as a report) that has to do with the case, which is addressed to the lawyer and given to him, may be presented because there is no privilege.

Civil Procedure Rules

Order 28 of the Civil Procedure Rules entitled 'Discovery and Inspection' affords a party a right to claim privilege over a particular document. More particularly, where an application for an order for inspection privilege is claimed for any document, it is lawful for the court or a judge to inspect the document for the purpose of deciding as to the validity of the claim of privilege. This right may be claimed for electronic documents that are deemed to be confidential, for instance the documents consist of personal communication between the party and a third party.

Order 28.3 of the Civil Procedure Rules provide that where a party is ordered to make discovery and fails to do so, he may not subsequently put into evidence any document unless the court is satisfied that he had sufficient excuse for failing to adduce the document when ordered by the court, in which case the court may allow the document to be put in evidence on such terms as the court may think fit. In addition, Order 28.12 of the Civil Procedure Rules provides that if any party refuses to allow inspection at the place named by him and within the prescribed time of any document that he has not objected to produce, or if he fails to comply with any order for discovery or inspection of documents, he is liable to attachment. He must also, if a plaintiff, be liable to have his action dismissed for want of prosecution, and, if a defendant, to have his defence (if any) struck out, and to be placed in the same position as if he had not defended, and the party seeking discovery or inspection may apply to the court for an order to that effect.

Protection of Confidentiality of Private Communications

A party may claim privilege by virtue of the Protection of Confidentiality of Private Communications (Interception of Conversations) Law of 1996 (the Confidentiality Law), which protects the confidentiality of a private communications. It follows from the above that a party may claim privilege on the basis of the Confidentiality Law for any form of verbal communication or telecommunication made by a person under circumstances where it is logical for that person to expect that it will not be recorded or intercepted by any other person, apart from the person intended to receive that communication. Protection will also be afforded for electronic communications that have been the subject matter of any unlawful interception private communications, that is without having acquired the previous express consent for the monitoring by the person who makes the communication as well as by the person who is intended to receive the communication or, in the case of immoral, disturbing or threatening anonymous telephone conversations, the consent of either one of the two parties.

Articles 15 and 17 of the Constitution

A party may also be able to claim privilege by virtue of Articles 15 and 17 of the Constitution of the Republic of Cyprus, which protect the Right of Privacy and the Right to Secrecy of Correspondence respectively. In addition, privilege may be claimed under Article 8 of the Convention for the Protection of Human Rights and Fundamental Freedoms, which is binding on the Cyprus legal system by virtue of Cyprus' international obligations.

Prevention and Suppression of Money Laundering Activities Law of 2007 and 2010

Where information is privileged, this cannot be disclosed in Court. Privileged information under this law means-

(a) a communication between an advocate and a client for the purposes of obtaining professional legal advice or professional legal services in relation to legal proceedings whether these have started or not, which would in any legal proceedings be protected from disclosure by virtue of the privilege of confidentiality under the law in force at the relevant time;

Provided that a communication between an advocate and a client for the purposes of committing a prescribed offence shall not constitute privileged information;

(b) any other information which is not admissible in court for the protection of the public interest under the law in force at the relevant time

Banking secrecy - Banking Laws of 1997 to 2009

«28A. (1) (a) All persons who carry out or have carried out a task on behalf of the bank and the auditors or experts commissioned by the Central Bank, are subject to professional secrecy.

(b) None of the confidential information that a person in subsection (1) becomes aware of, while carrying out his professional duties, shall not be disclosed to any person or any authority, except in a concise or collective form, so that the identity of the bank does not emerge, unless the case falls under the criminal law.

(c) Whenever a bank is declared bankrupt or its compulsory liquidation was ordered by the Court, any confidential information which is not related to the third parties who were involved in its rescue efforts is permitted to be disclosed in the context of procedures of the civil or commercial law.

(2) Irrespective of the provisions of subsection (1), the competent authorities of various Member States are not precluded from exchanging information in accordance with this Law and other laws or directives or regulations implemented by banks. This information is subject to the conditions of professional secrecy provided for in subsection (1). »

Other rules

Spouses: According to the Evidence Law, Cap. 9, spouses are able witnesses but they cannot be compelled to give evidence against their spouse unless they are also accused at the same time for the same crime with their spouse against whom they are giving evidence.

Conflict

The privilege of client-lawyer could be deemed to contradict with the Data retention law because the right to claim privilege will obstruct the disclosure of data before a 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?**

In the instances analyses under question 3 above, there are no specific provisions as to the manner in which public authorities are required to store the data obtained. Nevertheless, public authorities are required to maintain the data obtain sufficiently confidential.

The Protection of Competition Law of 2008

Section 33 of this law imposes a duty of secrecy for the protection of business secrets and confidential information:

«33.–(1) The Chairman, the other members and the substitute members of the Commission, the persons working under the supervision of the Commission, the staff of the Service and other public officers who by reason of their post or in the performance of their official duties obtain information on business secrets and information of a confidential nature, shall have a duty to secrecy and shall be bound not to communicate and/or publicize such information, except in so far as this proves necessary–

(a) to prove an infringement of sections 3 and/or 6 of this Law and/or Articles 81 EC and/or 82 EC of the Treaty;

(b) to implement the provisions of this Law.

(2) The same duty to secrecy shall be also owed by any other natural or legal person who obtains such information in the application of this Law according to the proceedings provided for in this Law.

(3) Without prejudice to section 38, violation of the duty to secrecy under this section shall constitute, in the case of public officers, a serious disciplinary offence punishable in accordance with the relevant disciplinary provisions.

(4) Nothing in this Law shall prevent the notification and/or publication of information for the purposes of applying the Community competition law. »

Banking Laws of 1997 to 2009

Disclosure of certain information.

28C.(1) Notwithstanding the provisions of subsection (1) of section 28A and section 29, the disclosure of certain information to other public authorities of the Republic responsible for the enforcement of legislation on the supervision of credit institutions, financial institutions, investment firms and insurance companies and to inspectors acting on behalf of those authorities. Such disclosures are made only where necessary for reasons of prudential control.

(2) The information received under subsection (1) of section 27 and sections 27A and 28A and information obtained by means of the on-the-spot inspections referred to in subsections (11) to (16) of section 27, may never be disclosed in the cases referred to in subsection (1), except with the express consent of the competent authority which disclosed the information or of the competent authority of the Member State in which on-the-spot inspection was carried out.

Banking Secrecy

Duty to maintain bank secrecy.

«29. (1) No director, chief executive, manager, officer, employee or agent of a bank and no person who has by any means access to the records of a bank, while his employment in or professional relationship with the bank, as the case may be, continues or after the termination thereof, give, divulge, reveal or use for his own benefit any information whatsoever regarding the account of any individual customer of the bank.

(2) Subsection (1) shall not apply in any case where -

(a) the customer or his personal representatives gives or give his or their written permission to do so; or

(b) the customer is declared bankrupt or if the customer is a company, the company is being wound up; or

(c) civil proceedings are instituted between the bank and the customer or his guarantor relating to the customer's account; or

(d) the information is given to the police under the provisions of any law or to a public officer who is duly authorised under that law to obtain that information or to a court in the investigation or prosecution of a criminal offence under any such law; or

(e) the bank has been served with a garnishee order attaching moneys in the account of the customer; or

(f) the information is required by a colleague in the employment of the same bank or its holding company or the subsidiary of the bank or its holding company or an approved auditor or legal representative of the bank in the course of their duties; or

(g) the information is required to assess the creditworthiness of a customer in connection with or relating to a bona fide commercial transaction or a prospective commercial transaction so long as the information required is of a general nature and in no way related to the details of a customer's account; or

(gi) the information is supplied for the purpose of maintaining and operating the Central Information Register set up under the provisions of sub-sections (3) and (4) of section 41; or

(h) the provision of the information is necessary for reasons of public interest or for the protection of the interests of the bank.

It is provided that the provisions of this section shall also apply to any branch of a bank from a member state established in the Republic, or to any bank which provides cross border services under the provisions of section 10A. »

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.**

According to the ***Report from the Commission to the Council and the European Parliament, "Evaluation report on the Data Retention Directive (Directive 2006/24/EC)***[2]

Statistics provided for either 2008 and/or 2009 indicate that the volume of both telecommunications traffic and requests for access to traffic data is less than 100 per year in Cyprus. Size of population, prevailing crime trends, purpose limitations and conditions for access and costs of acquiring data are all relevant factors.

On the basis of statistical breakdown provided by nine Member States, including Cyprus, for 2008 around ninety percent of the data accessed by competent authorities that year were six months old or less and around seventy percent three months old or less when the (initial) request for access was made.

Requests for retained traffic data by age in 2008

Age of data requested (months)/Cyprus

0-3 months: 30

3-6 months: 4

Total: 34

Requests for retained traffic data by age in 2009

Age of data requested (months)/Cyprus

0-3 months: 31

3-6 months: 8

6-9 months: 1

Total: 40

[2] http://ec.europa.eu/commission_2010-2014/malmstrom/archive/20110418_data_retention_evaluation_en.pdf

Requests for retained traffic data by type of data in 2008

Type of data

Fixed network telephony: 3 (0)

Mobile telephony: 31 (5)

Internet-related: 0 (0)

Total: 34 (5)

Requests for retained traffic data by type of data in 2009

Type of data

Fixed network telephony: 0 (0)

Mobile telephony: 23 (3)

Internet-related: 14 (0)

Total: 40 (3)

Requests for retained mobile telephony traffic data which were transmitted, by age, in 2008

Age of data requested (months)

0-3 months: 23

3-6 months: 3

Total: 26

According to another report located on:

www.dataretention2010.net/.../CY_Telecommunications_data_retention_law_additional_data.doc,

during the first semester of 2010, 15 Orders of Telecommunications Data have been issued by the Cyprus Police, as follows.

A/A	DISTRICT / DEPARTMENT	NUMBER OF THE ORDER
1	FINANCIAL CRIME UNIT	10/2010

2	FINANCIAL CRIME UNIT	14/2010
3	CID (OPERATIONS)	42/2010
4	CID (OPERATIONS)	46/2010
5	CID NICOSIA	09/2010
6	CID NICOSIA	11/2010
7	CID NICOSIA	18/2010
8	CID NICOSIA	19/2010
9	CID NICOSIA	22/2010
10	CID NICOSIA	23/2010
11	CID NICOSIA	25/2010
12	LAKATAMIA POL.STATION	03/2010
13	CID FAMAGUSTA	78/2010
14	CID PAPHOS	06/2010
15	CID LIMASSOL	27/2010

The above Orders concern eight cases in total, of which five have been detected while the remaining three are still undetected.

According to police investigators, the receipt and processing of telecommunications data that had been obtained from the Providers in three from the five detected cases, for which the court procedure has not yet been completed, has contributed, in some degree, to the detection of the said cases.

More specifically:

- During the investigation of the case of Illegal Transfer and Possession of Explosives, the fact that 2 Orders had been obtained and processed for this purpose, aided in the linking of the 3 suspects, since it had been established that they had telephone conversations between them.

- Moreover, in another case, which concerned the illegal use of data of bank cards, Orders of Access to Telecommunications Data had enabled the Police to discover the data of most holders / users of the specific IP Addresses, as well as the telephone numbers, to which the time of the conversations had been assigned, which was bought by the said credit cards. This resulted in the arrest and the prosecution of one person.

- Finally, in a case of Premeditated Murder, based on the telecommunications data that had been obtained, the testimony of the main witness was strengthened and some of the allegations of one of the defendants of the case were discarded.

B. Questions to the experts from only some of the Member States

7. Please describe the Supreme Court's decision of 1 February 2011 in the cases no. 65/2009, 78/2009, 82/2009 and 15/2010-22/2010 on data retention (essential reasons of the ruling, legal consequence).

The Supreme Court of the Republic of Cyprus decided on 1 February 2011 that Arts. 4 and 5 of the Law on the Retention of Telecommunications Data for the Investigation into Criminal Offences (L.183 (I) 2007) are in breach of the Constitution; moreover, the Law appears to go beyond the scope and goals of Directive 2006/24/EC on data retention.

The Court verdict was issued in relation to petitions for a writ of certiorari by four persons against District Court orders that granted the police access to the claimants' telephone communications data. The orders were issued according to Arts. 4 and 5 of L.183 (I) 2007 which aimed at harmonising Cypriot Law with the Directive.

The petitioners claimed that both the aforementioned articles of the Law and the District Court orders were in breach of the Constitution as they violated their rights of privacy and family life (Art. 15.1) and of secrecy of communications (Art. 17.1).

After an examination of the provisions of Directive 2006/24/EC, the Court deliberated that from both the title and the content of the Law it appeared that its goal was broader. While the Directive aims at the retention of descriptive communications data, the Law links the obligation for the retention of data not only to the investigation of serious criminal offences, but it additionally rules on issues regarding access to the data. At the same time, the Court noted that the legislator expressed through Art. 22 its will to maintain the existing state of affairs regarding the protection of the secrecy of communications. The case-law, which was created

in connection to the enforcement of the Law on the Protection of the Secrecy of Private Communications (monitoring of communications, L.92(I)/1996), was recalled by the Supreme Court, which noted that "monitoring or information that is connected to or comes from the communication between citizens and that falls out of the exceptions of Art. 17.2 of the Constitution cannot be accepted by the Courts as evidence"

The provisions of L.183 (I) 2007 on ways of access to telecommunications data by police authorities were introduced not for harmonisation purposes, since no such obligation on the Republic derives from Directive 2006/24/EC; therefore, they are not covered by Art. 1A of the Constitution, which establishes the superiority of EU directives over the Constitution. Thus, the Supreme Court examined the constitutionality of the relevant provisions, on the basis of which the orders on the disclosure of data were issued by the District Courts.

It found that:

a. Both the Constitution and Art. 8 of the ECHR protect privacy of communications, while case-law has established that any interference with an individual's telephone communication is a violation of his rights to privacy of communication.

b. Access to telephone call data by police authorities without the knowledge or consent of the persons affected constituted a breach of the secrecy of communications.

c. Access to telecommunications data was not a legitimate constraint on their right, since Art. 17.2 of the Constitution provides that such a limitation can only be imposed on convicted persons or such under pre-conviction or in the professional correspondence of bankrupt persons. At the time of the orders, one petitioner was free, therefore the orders infringed her rights; two petitioners were under pre-conviction. However, the orders allowed access to telecommunications data of periods prior to their arrest, which violated their rights; however no retroactive restriction was allowed by the Constitution or case-law. The fourth petitioner was serving a sentence of several years in jail and communicating via a mobile telephone was not allowed by law; therefore, he could claim no constitutional protection.

The Supreme Court issued writs of certiorari for the Courts orders concerning three of the petitioners and rejected the petition of the convicted person.

Please provide in particular answers to the following questions:

- Does the court sentence (*de iure* or *de facto*) have a general (*erga omnes*) binding effect or only does it only apply among the parties involved (*inter partes*)? If the first:

The court's decision has a general binding effect due to the fact that case law of the Supreme Court is considered to be 'precedent' under common law.

- What will happen to data that had been retained before the ruling? Is there an obligation to destroy these data?

The Court did not make an order as to the destruction of the data.

According to section 22 of the Data Retention Law, when it is ascertained with the consent of the Attorney General that the data obtained on the basis of a Court order are not connected to the commission of a serious criminal offence for which the order was issued, shall be destroyed within 10 days from the day that the Attorney General notifies his consent; the Supervising Authority shall be notified of the above.

- What will happen to data retained that had been requested by any of the entitled bodies (police etc)? May they be used by these bodies/in a court proceeding?

The same data cannot be used against the same parties as this would be against Art. 12.2 of the Constitution which provides:

"12.2. A person who has been acquitted or convicted of an offence shall not be tried again for the same offence. No person shall be punished twice for the same act or omission except where death ensues from such act or omission".

- Please describe how the legal situation the court sentence is based upon has changed as a consequence of the 6th Amendment to the Constitution. Would the Supreme Court be due to rule in a different way under the current legal status? If so: Please set out the differences that would be due.

The Supreme Court noted that in its deliberations it did not take into account the 6th amendment of the Constitution, that in certain cases allows an interference of the right of secrecy of communication by the authorities, since the orders were issued before the promulgation of this amendment (4 June 2010).

In order to better answer this question, a comparison of Article 17 of the Constitution is necessary, before and after its amendments.

The old version of Art. 17 used to read:

"ARTICLE 17 1. Every person has the right to respect for, and to the secrecy of, his correspondence and other communication if such other communication is made through means not prohibited by law. 2. There shall be no interference with the exercise of this right except in accordance with the law and only in cases of convicted and unconvicted prisoners and business correspondence and communication of bankrupts during the bankruptcy administration."

Article 17 was amended on the 4th of June 2010 by Law 51(I) of 2010 (the "Sixth Amendment of the Constitution") and currently provides that

"(1) "Every person has the right to respect for, and to the secrecy of, his correspondence and other communication if such other communication is made through means not prohibited by law";

(2) "There shall be no interference with the exercise of this right except in the following cases:

(a) convicted and non-convicted prisoners;

(b) following a court order issued in accordance with the provisions of the law following an application by the Attorney General of the Republic and the intervention consists in a measure which in a democratic society is necessary solely for the interests of the security of the Republic or for the prevention, investigation or sanctioning of certain serious crimes (such as murder, child pornography, trading in drugs, etc); and

(c) following a court order issued for the purposes of investigation of serious crimes sanctioned by imprisonment for a term exceeding 5 years and provided that the intervention concerns access to electronic communications traffic and location data and relevant data which is necessary for identifying the subscriber and/or user."

The aforementioned amending Law provides that the said amendment was enacted because according to the case law of the Supreme Court no person has the right unless authorized by the law for reasons prescribed by the Constitution, to monitor or interfere with the communications between citizens. In addition, the amendment was necessary in order to make possible the intervention where this is necessary for the purpose of securing the safety of the Republic as well as to prevent, investigate or sanction serious criminal offences.

Following the amendment of Article 17, the author believes that the Courts would take a different decision in the future.

In the decision of 1.2.2011, it was ruled that access to telecommunications data was not a legitimate constraint on their right, since Art. 17.2 of the Constitution provided that such a limitation can only be imposed on convicted persons or such under pre-conviction or in the professional correspondence of bankrupt persons. At the time of the orders, one petitioner was free, therefore the orders infringed her rights; two petitioners were under pre-conviction.

Following the amendment of Art. 2, the instances where a person's communication can be accesses have been broadened and extend beyond prisoners and bankrupts. Now data can be accessed where there is an investigation of a serious crime (where the sentence exceeds 3 years imprisonment) or for protecting the interests of the Republic.

- Does the ruling seek to strike a balance of the interests protected by fundamental rights and, where applicable, other norms enshrined in the constitution or having constitutional status? If so: which elements/aspects did the court consider when

trying to strike this balance, and what was the result of such assessment? Please explain the impact of the proportionality rule in this context.

The Court ruled that at the time that the orders had been issued, the Constitutional exemptions of Article 17.2 had not yet been implemented therefore it would be unfair to interfere with the right to secrecy of correspondence by using constitutional provisions that had not yet been adopted.

The Court did not refer to any other proportionality rule.

Please provide an overview of reactions of political and social groups to the ruling of the Constitutional Court (see question 7). Is it necessary/envisaged to table new legislation in order to bring national law in line with the Directive? If so: please describe, on the basis of questions 7 to 35 of the first questionnaire, how the legislative procedure and/or the public debate has evolved since the Court's ruling.

According to a statement of police spokesman Michalis Katsounotos to Cyprus Mail, "the decision will be studied in depth by the assistant police chief and all under investigation or criminal proceedings will be identified for which a court order was secured for the disclosure of telecommunications data, so that in consultation with the Attorney-general, a decision can be taken on the further handling of them."

"Unfortunately, the decision affects in a large and substantial way the work and mission of the police, particularly in relation to the outcome of major cases that are either in the process of investigation or in court," he added, noting that court orders were secured for the disclosure of telecommunications data in all those cases.

Katsounotos argued that it was in the public interest, particularly regarding "the sound administration of justice" for ways to be found for police to hold on to evidence collected to date on the basis of the existing law, which has now been declared unconstitutional.

This evidence was necessary in court, he said, adding, "we are confident that parliament and the Attorney-general will enter into consultations and do everything possible towards finding legitimate and effective solutions."

8. Please give your own opinion on the constitutionality of the data retention regime, as currently in force in your country, as a whole.

It would appear that since the enactment of the amendment of Article 17.2 of the Constitution, that the data retention scheme would be considered constitutional at least concerning the investigation of serious crimes and other public security reasons only.

9. **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?**

According to the Directive, the data to be retained are traffic data and location data and the related data necessary to identify the subscriber or user. The Constitution, Art. 17 does not specifically refer to types of data but to any communication in general. Therefore, the secrecy of correspondence can be interfered with only in those cases outlined in subsection (2) of Article 17 as analysed above.

10. **Please describe in detail which criminal offences are considered "serious criminal offences" in the sense of your answers to questions 15 and 16 of the first questionnaire.**

According to the Data Retention Law, section 2, a serious criminal offence is defined as a felony in accordance with the provisions of the Criminal Code or any other law or one which is sanctioned by a maximum prison sentence of five years and more or an offence which is specifically prescribed as a serious criminal offence in accordance with the provisions of the data Retention Law.

According to the Criminal Code, a felony is defined as a criminal offence punishable with 3 years imprisonment.

11. **Please describe the steps the entitled body has to take in order to obtain a court order prior to the data request. What will the court examine before taking a decision on whether or not to issue the order? Are there any situations (e.g. "emergency cases") that are exempt from the requirement of a court order? If so: who will decide in these situations whether or not access to the data may be requested? Is it necessary to have a court decide on the lawfulness of the access after the emergency situation is over?**

Police investigators must obtain the approval of the Attorney General of the Republic and on the basis of this approval, an application is filed before the competent Court for the issuing of a Court order enabling a police investigator to obtain access to data which are related to a serious criminal offence, in order to obtain evidence that a serious criminal offence has been committed.

<u>What will the court examine?</u>

An application for the issuing of a Court order must be made in writing, must be approved by the Attorney General and must be accompanied by an affidavit of the police investigator which must contain the following information (section 4(1) of the Data Retention Law):

(a) The full capacity of the police investigator;

(b) Full and substantiated account of facts and circumstances which forms the basis of the application, including:

(i) Details of the serious criminal offence that has been committed, is being committed or is expected to be committed;

(ii) General description of the period of time for which access to data is requested;

(iii) The identity of the person who committed or is expected to commit the offence;

(iv) The name, address and profession of all persons whose data is deemed reasonably important to be accessed in order to assist in the investigation of a serious criminal offence;

(c) A report on the time period required for accessing the data as well as a full description of the facts supporting a reasonable suspicion that other additional communication may be connected to such data to be accessed;

(d) A report on the facts concerning previous applications that have been filed for the purpose of issuing an order and which involve any other persons to whom the application is connected.

(e) A report on the outcome so far of the investigation or a reasonable explanation on the failure to receive such results where the application concerns an extension of the term of validity of the order.

A Judge may request additional details or information or evidence for the purpose of supporting the application in the form of an additional affidavit.

A Judge may issue the order authorizing access to the data if he is satisfied that on the basis of the facts that have been submitted:

(a) There is reasonable suspicion or possibility that a person has committed, is in the process of committing or is expected to commit a serious criminal offence;

(b) There is reasonable suspicion or possibility that specific data are connected or are relevant to a serious criminal offence.

Emergency situations:

According to section 4(2) of the Data retention Law, there is no requirement to obtain a Court order in the event that a person is kidnapped. In this case, the police investigator is entitled to obtain the data which is relevant to the investigation of the kidnapping by addressing a letter to the service provider. Before sending the letter, the police investigator must obtain the approval of the Attorney General and must set before the Attorney General certain information and data prescribed by the Data retention Law.

Within 48 hours from the date that the data has been accessed, the police investigator must obtain a relevant Court order. In the event that the Court refuses to issue the order, the police investigator is obliged to destroy the data collected within 48 hours of the Court's refusal.

12. **Please describe how – and how often – the exemptions to the notification obligation, mentioned in your answer to question 19 (for the purposes of the investigation, detection and prosecution of criminal offences), are applied by the Data Protection Commissioner in practice.**

    There is no public data available on this matter.

13. **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.**

    According to section 4(1) (d) of the Data Retention Law, for the purpose of filing an application for the issuing of a court order, a police investigator must file a report on the facts concerning previous applications that have been filed for the purpose of issuing an order and which involve any other persons to whom the application is connected.

    It can be assumed from the above that data to be retained may be the subject matter of various application for the issuing of a Court Order. No other rules are available on this matter.

14. **Has the Data Protection Commissioner, in the meantime, taken any "directions with regard to the degree of security of the data and to the measures of protection required to be taken for every category of data", as provided for by the Data Protection Law (see your answer to question 42 of the first questionnaire)?**

    No regulations or orders have been issued establishing such technical or organisational rules.

    If so: Are the technical and organisational measures standardised or specified in any other way, e.g. through guidelines issued by the supervisory authority? If so: Are these specifications binding or not for the bodies concerned? Please describe their content.

    In particular: do they provide for measures in one or more of the following areas:

    - physical protection of the data retained (e.g. through physically separated storage systems that are disconnected from the internet, located within particularly protected buildings)

- 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)

- rules on internal access restriction and control (e.g. four-eyes principle, secure authenification mechanisms/certificates)

- access logging

- secure (irreversible) deletion after expiry

- error correction mechanisms (e.g. hash functions, checksums)

- secure data transmission (cryptographic security, postal delivery)

- access/request procedure (transmission by the provider on request or direct access by the entitled bodies?)

- measures to ensure that data transmitted is used exclusively for the designated purpose (e.g. tagging through electronic signature, time-stamp etc)

- staff training/internal control mechanisms to ensure compliance with the law and other rules

- 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)?

15. Which public bodies are responsible for supervising that *the bodies entitled to obtain access to the data retained* (police etc) act within the law? Are these bodies independent in the sense of what has been said in question 35 of the first questionnaire?

The Data Protection Commissioner, established by virtue of the Processing of Personal Data (Personal Protection) Law, acts as the Supervising Authority

16. Which body is the "central authority" mentioned in your answer to question 44 of the first questionnaire with regard to the cooperation in criminal matters with the US?

The central authority is the Minister of Justice and Public Order or a person designated by the Minister.

17. As regards your answer to question 10 of the first questionnaire: according to the Order, is it a *right* or an *obligation* of the providers to store data for the

purpose of charging for services, payment of subscriptions and dispute resolution in relation to connection or billing?

It is an obligation.

18. **In your answer to question 25, you mention that *all* communications content is retained (point (a) of your answer). However, the requirement of a court order rather seems to point to a surveillance carried out on a case-by-case basis. Could you explain a little further how this systems works? If there is a blanket retention of all content, why was it necessary to introduce the mentioned amendment to the Constitution ("A Constitutional amendment in 2010 provides that the Attorney General can authorize phone tapping.")? Does the authorisation by the Attorney-General refer to the phone tapping operation as such or only to the access to communications content retained anyway?**

The answer under question 25 analysed the data that can be accessed under the Law for the Protection of Privacy of Private Communications (Monitoring Communications) of 1996, Law N. 92(I)/1996. This Law applies separately from and without prejudice to the Data Retention Law.

This Law protects the confidentiality of a private communication.

A private communication is interpreted as any form of verbal communication or telecommunication made by a person under circumstances where it is logical for that person to expect that it will not be bugged or intercepted by any other person, apart from the person intended to receive that communication.

Protection is also afforded to radio-communication, communication by wire and wireless means. A wireless communication is defined as any communication conducted by the use of facilities or telecommunications equipment for the transmission, broadcasting or receiving of points, signs, texts, pictures and sound or information of any nature with the aid of a wire, cable, or any other connection between the broadcasting and the receiving points which is made available, supplied or operated by CYTA (Cyprus Telecommunications Authority) or by persons authorised by CYTA.

The definition of communication given by the Law may also include e-mail and the Internet and thus the Law may also apply to these forms of communication.

'Interception of a communication' refers to the acoustic or any other form of receiving the content of any private communication with the use of any electronic, mechanical, electromagnetic, acoustic or other apparatus or machine and includes the hearing, magnetic taping or any other form of registration or receiving of the content of this communication either in whole or in part or with regard to its substance, meaning, importance or aim.

The term 'electronic, mechanical, electromagnetic, acoustic or other apparatus or machine' is defined as any apparatus or machine used or which may be used for the illegal bugging or interception of private communications. This does not include any

telephone or telegraphic equipment, tool or apparatus or telecommunications equipment or installation or facility or any of their components which is provided to the subscriber by CYTA or any other person who has a special licence by CYTA during their usual course of business.

According to this Law, a person will be guilty of an offence and will be liable to imprisonment up to three years if he/she:

(a) Taps or intercepts or attempts to tap or intercept or causes or allows or authorises any other person to tap or intercept any private communication, on purpose.

(b) Uses, attempts to use, instigate or causes or authorises another person to use or to attempt to use any electronic, mechanical, electromagnetic, acoustic or other apparatus or machine for the purpose of tapping or intercepting any private communication, on purpose.

(c) Reveals or attempts to reveal to any another person the content of any private communication, on purpose, while being aware or having reason to believe that the information was received by bugging or interception of private communication.

(d) Uses or attempts to use, on purpose, the content of any private communication, when being aware or having reason to believe that the information was received by tapping or interception of a private communication.

The provisions referred to above do not apply with regard to a person who:

(a) Registers numbers of telephone calls having previously ensured a court order or for the purposes of charging and the person who makes the communication is informed.

(b) Intercepts private communication after an authorisation or approval or bona fide assists another person to intercept a private communication where he has reasonable cause to believe that they are acting under authorisation or approval.

(c) Intercepts the private communication of persons communicating with third parties in prison.

(d) Is an officer, member or employee of CYTA or is a person who acts with CYTA's authorisation in such terms as CYTA has imposed and he is engaged in the provision of telecommunications services for the public and carries out the interception of private communication where this is accidental and absolutely necessary for the provision of such services or for the purpose of maintenance or control of the quality of telecommunications equipment.

(e) Is an officer, member or employee of CYTA, or is a person who acts with CYTA's authorisation in such terms as CYTA has imposed and has provided

information, facilities or technical support for the interception of private communication.

(f) Is a public officer who, during the exercise of his duties, has received knowledge of the content of the interception of private communication which has taken place according to an authorisation or approval granted by CYTA or another authority or testimony arising from such interception and has revealed this content to another officer. Provided that such revelation is absolutely confidential and it is necessary for the exercise of the official duties of the public officer who reveals it and for the public officer who receives it.

(g) Is a public officer who, during the exercise of his usual duties has received knowledge of the content of the interception of the private communication taken place after authorisation or approval or testimony arising from such interception and has made use of this content, provided that such use was absolutely confidential and necessary for the exercise of his official duties.

(h) Has received any information in relation to the interception of private communication or its content or testimony arising from such an interception and reveals their content while testifying as a witness at any criminal or civil procedure before the competent court, provided that the said interception took place according to the authorisation or approval granted by CYTA or another authority.

The above prohibition will also not apply where, inter alia, a person has the previous express consent for the monitoring of the private communication by the person who makes the said communication as well as by the person who is intended to receive the said communication or, in the case of immoral, disturbing or threatening anonymous telephone conversations, the consent of either one of the two parties.

19. With regard to your answer to question 55 of the first questionnaire: do you consider it possible that fundamental rights of the telecommunications providers other than the right to privacy (e.g. professional freedom or the right to property) may be infringed by the obligation to retain certain traffic and location data for the purpose of criminal investigation? If so, please provide an answer to question 55 of the first questionnaire in this respect.

No fundamental right or freedom of telecommunications providers appears to be infringed.

The relevant fundamental freedoms are the right to property (Article 23 of the Constitution) and the right to practice a profession (Article 25 of the Constitution). However, the Constitution provides for the right of the Republic to limit such freedoms where this is required for public safety or in the public interest.

Article 23:

"1. Every person, alone or jointly with others, has the right to acquire, own, possess, enjoy or dispose of any movable or immovable property and has the right to respect for such right... 2. No deprivation or restriction or limitation of any such right shall be made except as provided in this Article. 3. Restrictions or limitations which are absolutely necessary in the interest of the public safety or the public health or the public morals ... or for the protection of the rights of others may be imposed by law on the exercise of such right..."

Article 25:

"1. Every person has the right to practice any profession or to carry on any occupation, trade or business. 2. The exercise of this right may be subject to such formalities, conditions or restrictions as are prescribed by law ... are necessary only in the interests of the security of the Republic or the constitutional order or the public safety or the public order or the public health or the public morals or for the protection of the rights and liberties guaranteed by this Constitution to any person or in the public interest..."