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

Hellas

Grigorios Tsolias, Attorney at law, LLM (The replies are bounding only for the writer and do not express the opinion of any other private or public entity).

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

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

I. Legal provisions

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

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

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

Yes, Act 3917/2011 has implemented Data Retention Directive (DRD).

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

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

Please, see answer no 1.

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?

Please, see answer no 1.

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.

- ***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.

No, unfortunately there is not any. You can find the Act in Hellenic at http://www.ethemis.gr/3917-2011-diatirisi-dedomenon-pou-paragonte-i-ipovallonte-se-epexergasia-se-sinartisi-me-tin-parochi-diathesimon-sto-kino-ipiresion-klp/

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

The relevant regulations have been in force from 21 February 2011.

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

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

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

The relevant law has been voted by the members of the Parliament and has become an Act. All the legal provisions concerning data protection (e.g. Directive 95/46/EC), electronic communications (e.g. Directive 2002/58/EC and 2002/21/EC), security of electronic communications, Independent Administrative Authorities, obligations of the Providers (ISP's, CSP' s etc.) etc. have basically the legal form/type of an Act. In some cases, under the legal provision of an Act, it is given the authorization to issue a Presidential Decree or an Administrative Regulation, mainly for procedural, technical and organizational details. (E.g. under the current legal framework: the Presidential Decree 47/05, by authorization of Act 3115/03 for the legal interception of electronic communications, under the title "Procedure, technical and organizational guarantees for ensuring lawful interception" which provides the details for the procedure of both lawful interception (content of conversations) and access to traffic and location data, after a judicial order.).

The Act contains authorization to the competent Independent Administrative Authorities (Hellenic Data Protection Authority www.dpa.gr and Hellenic Authority for Communication Security and Privacy (A.D.A.E. – www.adae.gr) to issue Administrative Regulations concerning the obligations of the Service Providers for data protection and data security (art. 7 DRD) and for the storage requirements (art. 8 DRD).

The chosen types of legal acts correspond to those usually chosen in the Hellenic legal system for such kind of matters.

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 art. 2 par. 2 DRD are also referred to the Act and there is no difference between the two. Furthermore, the definitions in Directive 95/46/EC, 2002/21/EC and 2002/58/EC are applied also by reference to the Acts by which the above mentioned Directives had been implemented.

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?

Data that shall be retained are the same referred to art. 5 DRD. These rules do not include specific additional retention obligations with regard to traffic data that go beyond the obligations mentioned in the DRD, but in some rules of the Act there is a difference in the expression used, that could lead to a different interpretation on additional retention obligations or not. E.g. DRD's article 5 par. 1 (a) "data necessary to trace and identify the source of a communication" (2) "concerning Internet access, Internet e-mail and Internet telephony" has been transferred to the Act as "data necessary to trace and identify the source of a communication…concerning Internet access and via internet electronic mail and telephony services".

Data on unsuccessful call attempts have to be retained, provided that there is a connection to the Provider's system exactly as defined at art 2 section f' of the DRD.

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.**

    National law has implemented the legal provisions of 95/46/EC and 2002/58/EC where there is not a reference to any obligation of retention. However, there is the case of the retention of electronic communications e.g. the content of them and access to data when carried out in the course of lawful business practice (art. 5 par. 2 Directive 2002/58/EC), but not as an obligation.

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

    Access to stored data is allowed for the investigation and prosecution of particularly serious crimes. However, access to the stored data is permitted also for the national security reasons.

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)?**

    As far as "sensitive data" is concerned, Directive 95/46/EC, as implemented with Act 2472/97 is applied. Article 7A of the above Act stipulates that process of data from e.g. attorneys at law concerning legal services to their clients is exempted from the application of the Act and there is no need for any notification to the Data

Protection Authority or any prior permission, provided that the controller is bound by the attorney – client privilege.

Also, general rules for the protection of e.g. attorney-client privilege may apply. More specifically these rules are not referred to retaining of data. Actually, there is not a specific prohibition (or an exemption or special requirements) of intercepting the content of communication or accessing to communication data generated after a call between a lawyer and his client or other kind of requirements under which access may be ordered. If we are well informed about the German CCP, in Hellas there is not an article similar to article 160a of the German CCP.

According to Hellenic art. 100 par. 4 CCP «Under no circumstances the communication between the accused person and his lawyer is not allowed to be prohibited». According to the theory, the right of the accused person to a free communication to his lawyer means that this communication shall be secret and without the presence of any other person against the will of the accused person and the lawyer.

According to Hellenic art. 212 CCP the penal procedure shall be annulled in case that lawyers shall be examined as witnesses against their clients and unveil secrets that have learnt from them

According to Hellenic art. 261 and 262 par. 3 CCP (also Code of Ethics of Lawyers) confiscation of documents in a lawyer's office which are connected to article's 212 CCP professional secrecy is not allowed.

The above mentioned may lead to the conclusion that access to communication data that are generated after a confidential communication between a lawyer and his client is against the law and furthermore violates the defense rights of the accused person. On the other hand, the Hellenic jurisprudence has not yet accepted the above mentioned arguments, as far as we are informed.

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.**

Data shall be retained for a period of one (1) year.

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)?**

Access to the data retained is allowed to the law enforcement agencies, the security/intelligence authorities and the judicial authorities. More specifically:

a) Law Enforcement Agencies: Police (any kind of units: local police station, counter terrorism unit, special forces, military police etc.), Internal Affairs of Police, Coast Guard.

b) b) Security/Intelligence Authorities: Mainly the National Security and Information Services (www.nis.gr)

c) c) Judicial Autorities: Prosecutor, Inquisitor Judge, Judicial Council, Court.

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)?

According to art. 19 of the Hellenic Constitution access to communication data and to the content of communication is allowed only for reasons of national security or for the purpose of investigating particularly serious crimes (criminal offences), under the guaranties of the judicial authority (judicial permission), as specified by Act. The national laws shall not grant any right neither to individuals, nor the State to access the data in civil actions or administrative offences.

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)?

Requirements to access the communications data, are the same to these needed to access the content of a communication (lawful interception), meaning: a) for *particularly serious crimes*: justified suspicions, need of tracing the place of staying of the defendant, exhausting other means-ultimum refugium (finding the defendant is by any other means [than lawful interception or access to data], impossible or extremely difficult). These requirements are alternative. According to the Act 2225/94 surveillance in these cases is allowed only if the competent judicial council (or the prosecutor or the inquisitor judge in an emergency case) provides justification that solving the case or finding the place of staying of the defendant is by any other means impossible or extremely difficult and b) for *national security*: information or other elements which lead to estimation of danger for the national security (not justified or specific reasons or risks).

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?

It is required a decision either from the Judicial Council (consisted of three judges), or from the Court, or in case of emergency from the Prosecutor or the Investigating Judge. Where there is a court of first instance, there is also a Judicial Council, which deliberates in camera on all the issues falling within its competence. These include: supervision of the length of pre trial detention, resolving disputes between the investigating judge and the public prosecutor or the defendant for ordering the pre trial detention, orders of search or seizure, orders for lawful interception and access to communication data, orders for freezing bank accounts because of money laundering. This Council operates also as an indicting chamber in some cases by

deciding whether the defendant shall follow a trial or shall be acquitted without a trial.

In our case, the decision is secret and the target of the inquiry shall not be notified by the time of issuing the decision. It is not required to hear the aggrieved party, or to be more exact, it is forbidden to notify the aggrieved party.

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?

Lawful interception of communication's content and access to communication's data is a special investigating act, which is conducted in a secret way, meaning without the knowledge of the subject – person under investigation or his lawyer. The CDR's (Call Data Records = traffic and location data) either in hard copy (list in paper) or in an electronic way (CD-Rom) shall be sent to the competent Authority (e.g. Police) which asked the permission from the Judicial Council for the access. The Police e.g. shall continue with the processing of the data and will be led to specific evidence which will be the base for the criminal prosecution. The Police e.g. shall send all the evidence, including the communication's data to the Public Prosecutor who prosecutes the defendant. The defendant for the first time will be informed for the fact of the Police e.g. accessing the data when he will be informed of the criminal charges in front of the investigating judge and he will take a copy of the penal file.

Once he becomes a defendant, acquires all the rights for a fair trial. One of these rights is that he shall be informed of the nature and cause of the accusation against him and he shall have access to the criminal file against him. The accessed data shall be a part of the criminal file. Consequently the subject of the data (defendant) shall have access to the content of the criminal file and access to his communication data (as clues for the crime), once his attorney take copies of the penal file.

On the other hand, if the above mentioned investigation (including the processing of the communication's data) leads to the conclusion that there are not sufficient evidence against the subject of the data ("suspect") to be prosecuted, then the penal file shall go to the archive, no action shall be made and as a rule there is not any obligation to inform the subject of the data ("suspect") for the processing without his knowledge.

In the above both cases, notification of the access *may* be ordered (it is in discretion) by the Competent Administrative Authority, the Hellenic Authority for Communication Security and Privacy (A.D.A.E. – www.adae.gr) under two (2) conditions: 1) the investigation has been finished and 2) the purpose for which access to the data had been ordered is not annulled by the notification (art. 5 par. 9 Act 2225/94).

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

Please see reply no 18. Furthermore, in case of lawful interception against a third person (not a target, not a defendant e.g. the person with whom the suspect talks on the phone) the aggrieved party may be informed after the access and provided that the competent Independent Administrative Authority decide that there is a need to inform him.

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 aggrieved party (namely the defendant) may ask from the Judicial Council to annul the decision which allowed access to communication data, in case of non fulfillment of the requirements of the law or in case of violating the rights of the defendant (lack of fair trial). This procedure is regulated by the Code of Criminal Procedure as a general remedy for any kind of annulment and not specifically for the case of access to communication data. In case of an unlawful data access, the above mentioned procedure is also followed, but also there is criminal liability for the person who unlawfully accessed the data. Finally, the unlawfully accessed data may be excluded by the Court from evidence, after a petition of the defendant to the court. The Court is not obliged to accept the petition.

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.

There is *criminal liability* : a) sanction of imprisonment up to ten (10) years for the individual, b) sanction of imprisonment up to ten (10) years and a fine from 55.000,00 euros to 200.000,00 euros for the Service Provider (legal representative, member of the board, security manager etc.), c) sanction of imprisonment up to twenty (20) years and a fine from 55.000,00 euros to 300.000,00 euros in case of danger for the democracy or the national security and d) sanction of imprisonment from two (2) to five (5) years in case of negligence.

There is also *administrative* liability by imposing monetary sanctions (fines) from the competent Independent Administrative Authorities to the Service Provider (legal representative, member of the board, security manager etc.). Fines go up to 5.000.000,00 euros and there is also the fine of suspension or revoke of the services of the company.

The mentioned liability prerequisites in general terms a) intent of the perpetrator and (with the exception of negligence liability) b) violation of secrecy of correspondence (content or/and data) or violation of the security measures of the Provider or lack of security measures on behalf of the Provider.

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

The accessing bodies shall destroy the data transmitted to them within ten (10) days from the day of receipt of a court decision ordering so. According to the Act there is no automatic expiration day for the cases where after the decision of the Judicial Council, access to data has been allowed. In both cases (access to data and prosecution – access to data and finally no prosecution) the competent judicial authority shall order the destruction of the data within ten (10) days from the receipt of the judicial decision, which shall be issued by the end of the procedure (either end of investigation without prosecution, or end of the trial in the first instance, court of Appeal and Supreme Court).

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.

All the companies which fall into the definition of "provider of publicly available electronic communications service" (Directive 2002/58/EC and 2002/21/EC). This shall be a matter of interpretation of the definition by the Courts, in case there is a debate.

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?

It is a matter of the interpretation of the definition "provider of publicly available electronic communications service" because there is not a definition in the Act. This term is specified in the Act 3431/2006 under the title "Electronic Communications" (implementation of Directives 2002/19/EC, 2002/20/EC, 2002/21/EC, 2002/22/EC, 2002/7/EC) and specifically to art. 2: "the company which creates, functions, controls or provides network for electronic services or just provides electronic communication services". In fact, providers for the draft law shall be all the companies under the control of the National Regulatory Authority which regulates and supervises the telecommunications ("Hellenic Telecommunications and Post Commission – www.eett.gr). Providers in the meaning of the Act shall be considered all the companies under the control of the National Regulatory Authority.

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?

The Act specifically *refers to* all data categories exactly as the text of the Directive. According to Act 3471/06 (implementation of the Directive 2002/58/EC) there is a

reference to the terms "traffic" and "location data" without being analyzed - specifically referred as to the DRD.

For the purpose of the transmission of a communication, billing, interconnection payments, marketing, value added services etc. (art. 6 Directive 2002/58/EC) the data categories that have already been retained are not referred specifically at the law. In general lines under the current legal framework most of the mentioned at the DRD categories are retained, with the exception of the unsuccessful call attempts.

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)?

a) Yes, there is Act 3674/08 under the title "Reinforcement of the legal framework for privacy on telecommunications" which imposes security obligations to Service Providers. There are also the Administrative Regulations of the competent Independent Administrative Authority.

The telecommunication providers (sector of telephony only) are obliged to take the appropriate technical and organizational measures to safeguard security of its services, its premises, equipments, hardware, software and any kind of systems for publicly available telecommunications services. The provider is culpable for the security of its premises, equipments, hardware, software and any kind of systems for publicly available telecommunications services. The provider is obliged to have a *special security Policy*, following the Security Regulations of the competent administrative authority – A.D.A.E. This Policy shall be approved by A.D.A.E. This *special security Policy* contains: a) systems which shall be used for ensuring the secrecy of communications b) evaluation of the potential risks c) measures for prevention of risks. Act 3674/08 introduces the obligation of Providers to use cryptography for the voice signal of information in specific cases of transmission. It also introduces the obligation of the Providers to use a computer program of automatic registration of all the functions of the systems of the Providers. A.D.A.E. under the mentioned Act shall conduct audits and inspections of the Provider's premises, equipments etc. and the Providers are obliged to inform immediately ADAE, the public prosecutor and the subscribers in case of violation of the systems and secrecy of the communications. If the Provider shall not comply to the above mentioned obligations, administrative sanctions may be imposed by A.D.A.E. (see answer to question 21).

b) There is also the above mentioned Act 3431/06 implementing European Directives 2002/19/EC, 2002/20/EC, 2002/21/EC, 2002/22/EC and 2002/77/EC. Under the same Act, the above mentioned Regulatory Authority for the Communications and Posts ("Hellenic Telecommunications and Post Commission – www.eett.gr) is founded, which is competent for the quality and availability of the communications network.

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)?

There is not any estimation.

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?**

    No, there is no cost reimbursement.

    However, the Supreme Administrative Court (Hellenic Council of State – Conseil d' Etat) has recently issued its **4170/2011** decision, *annulling the non cost reimbursement provisions* of the Presidential Decree 47/05 for the legal interception of electronic communications, under the title "Procedure, technical and organizational guarantees for ensuring *lawful interception" which provides the details for the procedure of both lawful interception (content of conversations) and access to traffic and location data*, after a judicial order.).

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

    There is Presidential Decree no 47/05 and the Administrative Regulations of the competent Independent Administrative Authority for access namely to the lawful interception content of communications. Providers are obliged to give to the Authorities access to the communication and the data as soon as possible, provided that there is a judicial order.

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.**

    For the administrative and criminal sanctions, please see above replies under21. Civil liability (compensation) may arise because of moral or other damage. In that case the minimum compensation decided by the civil court shall not be less than 10.000,00 euros, unless the applicant asks for less.

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?**

    Public Authority (e.g. Police) contacts the Service Provider, refers to the judicial order which allows access and asks for the data. Under the current legal framework

and the current situation access to the content of communication is succeeded through L.I. electronic system, based on ETSI handover interface. Access to communication data is not electronic, but the Service Provider hands over in a CD ROM or in paper the data. Any dispute or any problem concerning access to retained data between Service Providers and Public Authorities may be solved by the competent Independent Administrative Authority.

The Competent Authority (A.D.A.E.) may solve the dispute in a way that is not considered similar to a Court's decision. A.D.A.E. may issue either an Opinion (which is not bounding), or a decision, which legally is an administrative act/decision/order and this may be challenged in front of the Administrative Courts, asking from any interested part its annulment. In case the same dispute leads also to a violation of the legal framework for the protection of secrecy of communications, A.D.A.E. may impose a fine.

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?**

    No, there are not.

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?**

    Act provides Administrative Regulations from the competent Independent Administrative Authorities.

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)?**

    Under the current legal framework, requests are issued by judicial authorities according to the European Convention on Mutual Legal Assistance in criminal matters. Schengen Treaty is also applied and especially article 53 which provides with the potentiality for the judicial authority to issue a request. In any other case, where the Schengen Treaty is not applied, article 457 – 461 Code of Criminal Procedure is applied, where the competence lies with the judicial authority. There is also use of www.ejn-crimjust.europa.eu (ATLAS system).

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)?

Hellenic Data Protection Authority and Hellenic Authority for Communication Security and Privacy which act under complete independence.

The mentioned Authorities act under absolute independence. Their members act under the same degree of independance as the judges. There is not any supervision from any Ministry, but their financial budget is part of the financial budget of Ministry of Justice. Every year the Authorities issue their Annual Report which is presented in front of the President of the Parliament. The only Authority which may audit (but not supervise) the above mentioned Authority is a special Parliament's Commission (consisted of elected parliament members of all parties) under the title "Commission for the transparency and institutions".

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?

No, there are not.

If so, please answer to the following questions:

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

/

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

/

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

/

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, there are not.

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?

Under the current situation, the data are stored at the Service Provider's premises and at a locally level.

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?

According to art 6 of the Act "the data referred to article 5 are generated and stored in natural resources within the Hellenic territory premises, within which (meaning the Hellenic territory premises) the data are retained for the purposes of the law for 12 months from the day of the communication".

Some Providers have implied that data are stored outside the country and according to the Press there had been discussions between the competent authorities because of a recent application of a world wide Provider asking to relocate all his Lawful Interception systems to another E.U. country.

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

a) no data are retained beyond what is permitted?

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

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

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

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

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

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

All the technical and organisational measures shall be taken after issuing an Administrative Regulation from the competent Independent Administrative Authority.

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

The requirements for the effective control shall be a part of the above mentioned (please see reply no 40) Administrative Regulation.

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

The technical standards shall be a part of the above mentioned (please see reply no 40) Administrative Regulation.

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.**

Please see reply under 40.

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?**

Please see reply under 34. In this context the English language is used.

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).

Yes, society is aware of the public surveillance measures. There is not a wide public debate. Some civil rights groups have been opposed to the DRD. Also some political parties.

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)?

There is not an obligation to retain other personal data and the PNR agreement has not yet been enacted.

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.

No, there are not.

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, there is not.

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 is a discussion to make easier access to the communications data by issuing an order from the Public Prosecutor, without the intervention of the Judicial Court.

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?

Article 9 of the Hellenic Constitution states: "Privacy and family life of each one is inviolable".

Article 9A of the Hellenic Constitution states: "All persons have the right to be protected from the collection, processing and use, especially by electronic means, of their personal data, as specified by law. The protection of personal data is ensured by an independent authority, which is constituted and operates as specified by law".

Article 19 par. 1 of the Hellenic Constitution states: "Secrecy of letters and all other forms/means of free correspondence or communication shall be absolutely inviolable. The guaranties, under which the judicial authority shall not be bound by this secrecy for reasons of national security or for the purpose of investigating particularly serious crimes, shall be specified by law". Restrictions on the inviolable right to the privacy/secrecy of article 19 par. 1 Constitution may be ordered only pursuant to the law and under the guaranties of the judicial authority. Such laws are: a) Act 2225/94, as amended by Act 3115/03, b) Act 3471/06 and c) Presidential Decree 47/05.

"Under the guaranties of the judicial authority" is the exact wording (in translation) of article 19 of the Constitution. It means that communications secrecy (both access to content and data) of any citizen (even the perpetrator of an offence) is valid against anybody, except the competent judicial authority, which has the right to issue an order by which this secrecy is seized. It also means that no one (e.g. Police, Ministers, Army, the President of the country) besides the Judicial authority, has the right to access to communications. In Hellas the judges are considered to be a guaranty for any restriction of rights. For example, a house search is forbidden to be conducted by the Police, unless a judge is present at the time. In the same way, access to communications is forbidden to be done by any one, unless a judge orders so. The "guaranties of the judicial authority" means that the judge, regardless of the absence of the perpetrator or his lawyer is obliged to protect his rights and the human rights of any person.

In our opinion data retention shall affect also other fundamental human rights, such as the right of each person to develop his personality, to live in honour and liberty (article 5 of the Hellenic Constitution), also the right that the value of a human being should be respected and protected by the State (article 2 of the Hellenic Constitution). The fact that these data shall be retained regardless of the liability of each human being for a potential crime in the future, violates primarily the right to

[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).

develop his personality and live in honour because he is considered as a potential criminal. Data retention implies that all the human beings are potential future criminals and furthermore without any specific reason. A defendant for a criminal offence, at least has the right to be presumed innocent until proved guilty. In the data retention case, the user of electronic communication services is not a defendant, but he is actually considered as suspect.

The fundamental rights mentioned above result from the Hellenic Constitution.

In the past, there has been a legal debate whether article 19 par. 1 Hellenic Constitution applies not only to the content of communication, but also to the communication data (traffic and location). This legal debate finished by issuing Act 3471/06, which implemented Directive 2002/58/EC and provides that communication data may be accessed under the same requirements and the same procedure as the access to the content of an intercepted content communication. Data which are considered as telecommunication content are data which may unveil information about the fact, about the essence of the communication, e.g. which internet/web site the user visited. Access to communications data and content require their retention. Article 19 of the Hellenic Constitution allows access to these information only for two (2) reasons: for reasons of national security or for the purpose of investigating particularly serious crimes.

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?

Article 25 par. 1 c. d' of the Hellenic Constitution states that "Restrictions of any kind which according to the Constitution may imposed to upon human rights, should be provided either directly by the Constitution, or by statute, should a reservation exist in the latter's favour, and should respect the principle of proportionality". E.g. the right to the secrecy of communications under article 19 of the Hellenic Constitution is restricted for reasons of national security or for the purpose of investigating particularly serious crimes, under the guarantees of the judicial authority and under the requirements of the competent Act.

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?

No, there is no jurisprudence.

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?

Article 19 of the Hellenic Constitution allows the restriction of the fundamental right of the secrecy of the communications only for national security reasons and for

investigation of extremely serious crimes. That means that the legislator has already assessed/balanced in article 19 the need to protect human life, fortune, public safety as a value more important than the secrecy of the communication in the specific case where a person is accused for violating the laws. This means that article's 25 par. 1 d' of the Hellenic Constitution "principle of proportionality" has already been taken into account in article 19. Furthermore, the judge shall apply the "principle of proportionality" in each case, beyond the wording of article 19.

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)?

Access to communication data, under the above mentioned interpretation of art. 19 of the Hellenic Constitution (please see reply 50 at the end) requires retain of the data. Access to communication data is allowed only for national security reasons and investigation of serious crimes. Except these two (2) categories, every other obligation to access communication data is contrary to the Hellenic Constitution, as above interpreted.

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?

Please see reply under 50. Furthermore, we have to differentiate retention obligation from accessing and processing the retained data. Under the Hellenic current legal framework and the Act the data should be retained in secure databases and accessed only after a judicial order for a specific reason (particularly serious crime). If the data are not accessed, they should be deleted after one year. Consequently, there is a debate whether is an affect or not concerning a restriction on other fundamental rights (e.g. professional freedom) when the data is conserved in a database and no one has access to these.

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)?

Service Providers are obliged to retain and hand over the asked data, exactly as described in the judicial order. Service Providers are obliged to hand over only the retained data for the purposes of the Act only.

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

It is a matter of interpretation. In our opinion private sector (Service Providers) shall not be neither the "long hand of the State", nor they shall be obliged to help the State for free, as long as their aim is to gain profits.

According to article 4 par. 5 of the Hellenic Constitution Hellenic citizens contribute to the public burdens proportional to their financial potentials (Principle of equality of public burdens)

According to article 5 par. 1 of the Hellenic Constitution everyone shall have the right to participate in the social, economic and political life of the country, insofar as he does not infringe of others or violate the Constitution.

According to article 17 par. 1 of the Hellenic Constitution property is under the protection of the State. Under the jurisprudence of the ECHR in the meaning of property is not only the land but a series of assets (see also art.1 Protocol no 1 to the Convention for the Protection of Human Rights and Fundamental Freedoms).

According to article 78 of the Hellenic Constitution every fiscal burden should be imposed by a specific law. Hidden taxes are not allowed (Principal of legality of imposing taxes).

According to the interpretation, first of all there is a violation of the right to the property and the right to the freedom of participation to the economic life when the State takes advantage of the fact of the agreement for providing services (agreement between the Provider and the user/subscriber) and asks from the provider in the basis of this contract (that has nothing to do with the State) to extent the services to the State for free. E.g. there is a debate about this matter in Hellas, in case the judicial order contains the obligation towards the Provider to assign to an employ (or more) in a 24hs base, the task to immediately inform the Police about any change of the location of the suspect (based on the location data which may be generated at any time of the day). This obligation has an extra cost for the Provider which furthermore cannot decide by his own whether he is going to use e.g. 100 employs or 103 employs, because of the obligation to add to his staff more employs for 24 hours a day just to serve the purposes of the State.

The above mentioned violation leads also to a potential violation of Article 49 of the EC Treaty prohibits restrictions on the freedom to provide services within the Community.

Furthermore, if the State does not reimburse the costs and the Provider is obliged to carry all the costs, then the amount paid consists a hidden tax and that is opposite to the principle of equality of public burden, principle of legality of imposing taxes and to principle of proportionality

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?

Article 28 par. 1 of the Hellenic Constitution stipulates that the rules of international law and of international conventions shall prevail over any contrary provision of the Hellenic law.

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

There is the legal obligation to implement a Directive and become a law of the State. Usually the competent Minister decides the institution of a Special Scientific Legislative Committee which draws the draft Act. This draft Act should be examined by the competent committee of the Hellenic Parliament, should be examined by the scientific legislative committee of the Hellenic Parliament and finally should be discussed and voted by the members of the Hellenic Parliament. It is possible to transpose a Directive through an Act, a Presidential Decree or a Ministerial Act.

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

No, it does not.

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?

Act provides that article's 9 Supervisory Authority should be two (2): Hellenic Data Protection Authority and Hellenic Authority for Communication Security and Privacy, which are Independant Administrative Autorities.

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

Hellenic Constitution does not set any limit.

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 number of the Public Services that have access to the retained data should be minimized. In case of access to data for national security reasons, there should be a prior control by an Independent Authority.

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

Hellas

Grigorios Tsolias, Attorney at law, LLM (The replies are bounding only for the writer and do not express the opinion of any other private or public entity).

Part 2: Overarching issues and country-specific questions

A. Questions to the experts in all Member States

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

No, constitutional law does not provide for a right to communicate anonymously, but it also does not prohibit it.

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?

Because of the recent Act 3917/2011 (21-02-2011 day of publication of the Act) there is no discussion for any amendments. On the other hand, there are some groups for the protection of human rights having expressed individually the opinion that the DRD leads to the end of the right to privacy as a whole, without specific legal objections or propositions.

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?**

   Data retention for the investigation, detection and prosecution of criminal offences is the only legal tool through which the private actors can be obliged to provide with information concerning electronic communication data.

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

   First of all, please see answers to the first questionnaire.

   Furthermore, according to art. 273 par. 2 CCP the accused person has the right of silence and the right of non self incrimination.

   According to art. 223 par. 4 the witness has the right to refrain from any reply which should led to his self incrimination.

   The meaning of the right of silence and the right of the non self incrimination contains the right not to deliver any kind of evidence (documents, list of communication data, telephone bills etc.).

   These rights to refuse to testify, does not conflict with data retention in a way that they bar these data from being retained, transmitted or used as an evidence in court because the above mentioned right of non self incrimination has to do with any evidence that the person its self is obliged to provide. In data retention case, the evidence (namely the communication retained data) is given to the Authorities (e.g. the Police or the Court) by the Service Providers.

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

   The Competent Independent Authorities for the application of the security measures shall publish Security Regulations. These Regulations containing the measures are not yet published.

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.**

   No, unfortunately there are not.

B. Country-specific questions

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

   Obligatory data retention for a specific duration of time for reasons of investigating, prosecuting and detecting criminal offences against every user of electronic communications, regardless of committing a crime or not, sets a series of legal matters. By retaining all the communication data because of the possibility that a citizen in the future may commit a crime, makes everybody of us a potential suspect. But the meaning of the word "suspect" has as requirement the commitment of a crime. In data retention, all the communication data is kept, not because a crime is committed and we shall investigate to find who the suspect or the perpetrator is, but because a crime may be in the future shall be committed. Or not. In this aspect, we all are "suspects" of a crime that has not yet been committed. This violates the constitutional right of a citizen to respect and protection of the value of the human being (art. 2 par.1), to develop freely his personality (art. 5 par. 1 Hellenic Constitution) and the right to enjoy full protection of his life, honour/dignity and liberty (art. 5 par. 2 Hellenic Constitution).

   What options for improvement do you see in terms of balancing the interests of freedom and security in the context of data retention (see question 63 of the first questionnaire)?

   I think the Hellenic Act has balanced the interests of freedom and security and there is no need for serious improvements, based on the DRD. However, there should be an improvement on the general legal framework for the lawful interception and access to communication data.

8. **Please explain in which points Act No. 3917/2011 ("the Act"), adopted on 21 February 2011, differs from the draft version referred to in your answers to questions 7 to 35 of the first questionnaire (please reply question by question).**

   There is no differentiation to the questions, except from:

   - Q13: Act provides for a data retention period of one (1) year.

   - A very important differentiation has to do with art. 6 of the Hellenic Act under the title "Duration and premises of data retention" where the law inserts the obligation of the Service Providers to retain the data exclusively in the territory of Hellas.

When answering, please consider the following remarks:

- **on Q11 of the first questionnaire: Your answer referred to the purposes of *access* to the retained data, whereas the question refers to the purposes for *retention* (as opposed to Q15). Are there any such purposes mentioned in the law?**

  According to art. 1 par. 1 Act 3917/2011 Service Providers are obliged to retain the data of article 5 with the purpose to give access (to the data) by the competent Authorities (Police, Judges etc.) for investigating, prosecuting and detecting criminal particularly serious offences.

- **on Q16: please specify the catalogue of criminal offences falling under the term of "particularly serious crime".**

  Article 4 of Act 2225/94 under the title "Lawful Interception for the investigation of particularly serious crimes" provides in **par. 1** that lawful interception (and access to retained data according to art. 1 par. 1 Act 3917/11) shall be conducted for the (pre trial) criminal investigation of offences which are exhaustively listed in the statutes of this paragraph (no 1), mainly felonies (punishable mainly by custodial penalties, mainly by a term of 5 years to 20 or by life imprisonment):

  a) Penal Code: high treason, attempt to murder the Prime Minister etc. political persons, torture and violations of human dignity, treason against the state (actions against State security, rendering military services to enemy services, revealing state secrets, espionage, forgery or concealing or destruction of documents against State interests), offences relating to the free exercise of civil rights (violence against Parliament, members of Parliament or members of Government to avoid or to be obliged to action, bribery), offences against public order (criminal organization-see also article 253A Criminal Procedure Code for criminal organization and terrorism), offences relating to currency (counterfeiting and setting into circulation coins and banknotes), offences relating to civil servants (bribery of servants in public or municipal utility companies, judges), offences relating to common danger (arson, explosions, disabling safety devices in factories or mines), offences against security in transportation (aviation, railway and water transportation), offences against human life (homicide), offences against personal freedom (kidnapping), offences against sexual freedom and relating to the economic exploitation of minors and child pornography, offences against property (theft, robbery), offences against property rights (blackmail). Furthermore, lawful interception may be ordered in case of the offence of planning to commit counterfeiting of banknotes or coins, offences relating to antiquities, child pornography and sexual abuse of minors.

  b) Special Penal Acts: Military Penal Code for specific crimes, trafficking weapons, illegal drugs trafficking, violations of Customs and Taxes Laws, bribery of foreign servants in public services (Act 2656/98), Act 2803/00 on the protection of the financial interests of E.C., money laundering, internal affairs of

Police, offences related to the Stock Market, Coast Guard Act, Penitentiary/Correctional Act.

- **on Q17 to 20: your answers seem to refer exclusively to the situation that data is accessed for criminal investigations. Please also add details on the rights of the data subject in the case that data is accessed for national security purposes.**

  Access to retained data for national security purposes is ordered be the Criminal Prosecutor of the Court of Appeal after an application of a Judicial, Political, Military or Police Authority. The Prosecutor decides to order or not the access within 24 hours. The order contains the name of the Authority which asked the access, the purpose of the access, the name of the Provider and the communication elements, the place and the duration of the access. Under a special request of the Authority which asks access to data, some of the above mentioned details may be not be referred or be referred not in details.

  In some cases, national security reasons may connect to criminal offences such as e.g. criminal organisation. In that case, may be the investigation has started as a national security matter, but finally ends as a common criminal offence. In that case, the subject has all the rights referred for the investigation of criminal offences.

  If access to retained data is ordered for exclusively national security purposes which are not connected to a criminal investigation, the subject is not notified and most probably, shall never be notified of the surveillance and access to data against him. According to art. 5 par. 9 Act 2225/94 in connection to Act 3115/03 the Competent Independent Authority (A.D.A.E.), which is informed for the surveillance and access to data has the right to after the end of the taken measure to notify the subject, if the purpose pf the measure is not under danger by this notification. The same legal statute, gives, in my opinion, the right to any citizen to ask the A.D.A.E. if he has been under surveillance and if his data has been accessed.

9. **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? Which cases are to be regarded as "emergency cases" so that access to the data may be sought by the Prosecutor or the Investigating Judge? Is it necessary to have a court decide on the lawfulness of the access after the emergency situation is over?**

   According to Hellenic **Act 2225/94** for the interception of communications and access to data, what you refer as "court order" is given by the Judicial Council, as a rule. The reference to the Judicial Council, the Investigating Judge and the Prosecutor has to do with the investigation of the crime, meaning the period before the trial in front of the court. Especially:

   Article 4 provides in **par. 2** that lawful interception (and access to data) shall be ordered only if during the criminal investigation, the competent Judicial Council

(consisted of 3 judges) issues a justified decision (order) declaring that the investigation of the case or tracing the place of staying of the defendant is by any other means (than lawful interception) impossible or extremely difficult. The Council should refer to all the facts of the case and the evidence provided by the request Authority (witnesses, documents etc.) and justify the reason why is necessary to grant access to data and the reason why the use of other means has until that time where unsuccessful.

Article 4 provides in **par. 3** that lawful interception (and access to data) shall be ordered against a specific person or persons connected to the case under investigation or for other persons, who (based to particular facts) are considered to take or carry messages from or to the defendant or are his contacts.

Article 4 provides in **par. 4** that lawful interception (and access to data) shall be ordered by the Judicial Council of the First Instance or by the Judicial Council of the Court of Appeal of the area where the offence has been committed. During a trial, the Court may function as a Judicial Council to order access to data.

Article 4 provides in **par. 5** that the request to the Judicial Council for the lawful interception (and access to data) is submitted by the Public Prosecutor or by the Investigating Judge for the offence under investigation or preliminary inquiry. The Judicial Council issues a decision within 24 hours, accepting or rejecting the request. Especially for the offences relating to the Exchange Stock Market, the Capital Market Commission shall ask the Public Prosecutor or the Investigating Judge to submit a request to the Judicial Council.

Article 4 provides in **par. 6** that the Investigating Judge and the Public Prosecutor (who carries out the investigation or the preliminary inquiry) shall be entitled to issue an emergency (provisory) order for lawful interception (and access to data), which is immediately enforceable, but immediately thereafter, he shall submit within 3 days a request to the Judicial Council to confirm or cancel the order. The validity of the emergency order expires after 3 days, unless the Judicial Council confirms the order.

An emergency case may be e.g. the case that there is an arrested suspect and within 5 days the Investigating Judge is obliged to decide whether he shall set him free, or order his custody, after having considered the evidence.

Article 5 under the title "Procedure for lawful interception" provides for the content of the judicial order for the lawful interception due to national security reasons in **par. 1** and for the investigation of particularly serious crimes in **par. 2.** The Judicial Order accepting the request, according to **par. 2,** contains: a) Judicial Authority (public prosecutor, or investigating judge or Judicial Council), b) Requesting Authority (public prosecutor, or investigating judge etc.), c) the reason for taking the measure, d) the Communication Service Provider which is ordered e) place and time of the measure f) date of issuing the order g) the name of the person or persons whose communications shall be intercepted and their address if known h) reasoning of the decision.

The Judicial Order denying the request, according to **par. 3,** contains: a) Judicial Authority b) Requesting Authority c) date of issuing the order.

The Judicial Order accepting the request for the lawful interception shall be served: to the competent independent administrative Authority (A.D.A.E.) and to the Communication Service Provider, according to **par. 4** of the article 5.

After the enforcement and execution of order by the Service Provider, the requesting authority shall draw up a report containing: all the actions made for the lawful interception, the place, the date and the procedure, the names of the employees, if necessary, according to **par. 5.**

Lawful interception (content of communication) for particularly serious crimes shall be ordered, according to **par. 6**, for a time period of 2 months starting from the day of issuing the order. It may be prolonged for no more than 2 months each time, under the same procedure, provided the necessity of continuing the interception. The maximum period of prolongation shall not exceed 10 months. This provision is construed as obviously referring merely to the content of communication.

Lawful interception procedure shall be ceased either upon the end of time period referred to the judicial order, or upon the expiry of the maximum time period, according to **par. 7**, or previously, in case the aim of the measure shall be fulfilled or shall be no more need, according to **par. 8.**

Article 5 **par. 9** provides that the information gathered through lawful interception during the execution of the judicial order shall be delivered to the requesting Authority, shall be included in the criminal case file against the defendant and shall be used for the aims of the criminal prosecution. If the information is irrelevant to the case under investigation, the competent Independent Authority (A.D.A.E.) may decide to inform the persons whose communications were intercepted for this fact, and then the Judicial Council may order the redelivery of these information to the persons whom they concern. Otherwise, the judicial council shall order the destruction of the said information, before the requesting authority and a record in writing shall be made as a proof for the destruction. In any case, the Judicial Council shall order the destruction of the information which was irrelevant to the aim of the order gathered through lawful interception.

Article 5 **par. 10** provides that the intercepted content of communication (gathered during the execution of the judicial order) and any other related data shall not be used as an evidence (directly or indirectly) in the context of a different criminal, civil, administrative or disciplinary trial or even administrative procedure and for an aim other than the one contained in the order. Exceptionally, the Judicial Authority which issued the order may issue a new order, permitting the use of information, if necessary, for the investigation of another particularly serious crime and for the defense of the defendant.

Article 5 par. **11** provides for the penal sanctions for the employees of the Service Provider who shall not comply with the judicial order by means of not providing to the competent authority technical assistance or information ordered (by the judicial

council) to be provided. Furthermore, penal sanctions shall be imposed on any employee of the Service Provider who shall disclose to third parties (non-authorized) the content of the communication that he learnt because of his office.

10. **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.**

    No, there are not such rules.

11. **Please give more details about how EU legislative acts and international treaties on cross-border co-operation in data retention issues (including both rules specifically designed for data retention as well as general rules applicable to data retention) are applied in your country. May data be accessed directly by the entitled bodies?**

    There are not specifically rules for data retention. Please see answer 34 on the first questionnaire.

12. **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 supervisory bodies independent in the sense of what has been said in question 35 of the first questionnaire?**

    Yes, the two mentioned Independent Authorities.

13. ***Once the administrative regulations mentioned in the Act have been adopted* (according to Art. 7 para. 2, 8 para. 2 of the Act, this shall happen within 3 months of the entry into force of the Act): please answer questions 38 to 44 of the first questionnaire. Which of the big providers have already drawn up specific security plans for the technical and organisational implementation of the data protection and data security requirements, as provided for by the Act? Please provide an overview of the content of these security plans.**

    The administrative regulations have not yet been published.

14. **Please describe the rules for co-operation among the different bodies accessing the data and between these and other public authorities in detail. Are there any provisions that allow the bodies entitled to obtain access to the data retained to transfer these data, once obtained, to other authorities for their respective purposes? If so, please describe the requirements that have to be fulfilled for such transfer.**

    Act 3917/2011 does not contain any rule. On the other hand, Act 2225/94 for the interception of communications and access to data stipulates on **art. 5 par. 10** that the content of the communication and the accessed data after a judicial order is forbidden as a rule, under the penalty of annulment of the judicial procedure, to be used and be evaluated as an evidence in front of another procedure of a criminal,

civil, administrative, disciplinary trial or administrative procedure for a different purpose than the one for which it had been ordered. Exceptionally, the Authority which ordered the interception of communications and access to data, may give a supplementary further justified order, upon request, for the use of the same evidence (content of communication and/or retained data) for another criminal case, under the requirements of the same law and for the exercising of the defense right of the accused person in a criminal trial.

15. Please explain the content of the *general* provisions on data protection and data security in electronic communications according to Act No. 3674/08, as far as they apply to data retention besides the specific provisions mentioned in question 13.

The administrative regulations referred to article 7 of Act 3917/2011 have not yet been published.

The administrative regulation of Act 3674/08 is not yet in force.