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

Portugal

Carlos de Almeida Sampaio/Inês de Sá

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. Law 32/2008, of 17 July (hereinafter, "Law 32/2008"), transposed to the Portuguese legal order Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006, on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks (hereinafter, "the Directive").

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

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

   Not applicable.

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

   Not applicable

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

   Not applicable.

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

General questions

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

   It is possible to find an English version of Law 32/2008 on the website of ANACOM (*Autoridade Nacional de Comunicações*) which is the Portuguese communications regulator (URL: <u>www.anacom.pt</u>).

   Please note, however, that the text available is not an official translation of the law.

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

   According to its article 18, Law 32/2008 took effect 90 days after the publication of Administrative Rule 469/2009, of 6 May (hereinafter, Administrative Rule 469/2009). Therefore, Law 32/2008 came into force in 5 August 2009.

   Administrative Rule 469/2009 laid down the technical and security conditions under which electronic communications for the transmission of traffic and location data on natural personas and legal entities, as well as related data necessary to identify the subscriber or registered user, must operate, pursuant to Law 32/2008.

   An initial trial period of 3 months which lasted until 30 November 2009 was established and further extended for another 6 months in order to address the functionality and usability of the software created for this purpose (the "SAPDOC"),

as well as to enable a steady adjustment of professionals to the new working procedures.

A new trial period started on 17 August 2010, which shall only expire upon joint order of the members of the Government responsible for the internal administration and justice areas.

Therefore, as a matter of fact, the transition period is still running in Portugal.

But in the course of this trial period, requests for data retained and replies from the providers which are not submitted through such software (the "SAPDOC") shall be carried out in the traditional way (e.g. mainly CD-ROM and paper).

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.

Law 32/2008, which transposed to the Portuguese legislation the Directive, is an act approved by the Portuguese Parliament. It governs the retention and transmission of traffic and location data on both natural persons and legal entities, and of the related data necessary to identify the subscriber or registered user, for the purpose of the investigation, detection and prosecution of serious crime by competent authorities.

Later on, four Administrative Rules, which are regulatory provisions establishing internal instructions about the enforceability of lawmaking acts such as Law 32/2008, were approved in connection with this act:

Administrative Rule 469/2009, of 18 August, laid down the technical and security conditions under which electronic communications for the transmission of traffic and location data on natural persons and legal entities, as well as of related data necessary to identify the subscriber or registered user must operate, pursuant to Law 32/2008.

Administrative Rule 915/2009, of 18 August, established a trial period of 3 months (up to 30 November 2009) in order to address the functionality and usability of the software later designated as "system of access to or request of data from communication operators" (the "SAPDOC").

Administrative Rule 131/2010, of 2 March extended such trial period for another 6 months, starting 1 December 2009.

Finally, Administrative Rule 694/2010, of 16 August (hereinafter "Administrative Rule 694/2010"), amended the initial version of Administrative Rule 469/2009. The subject-matter of the initial version of Administrative Rule 469/2009 was broadened so that it now also establishes the communicating method by electronic means of any lawful request for data storage or transmission made by the court or any competent agent under the law to providers of publicly available electronic communication services or of public communications networks, in the scope of criminal proceedings or of criminal investigations or inquiries.

The most relevant issues resulting from the transposition of the Directive are contained in Law 32/2008, a legal diploma of the responsibility of the Portuguese Parliament.

The four administrative rules aforementioned were approved by the Ministries for Internal Administration, Justice and Public Works, Transport and Communications and are considered to be acts of regulatory, not legislative, nature since they deal with issues of technical order. The provisions contained in the administrative rules seek to determine how the provisions of Law 32/2008 are to be technically implemented. Administrative rules have, however, the force and effect of law since they are binding as well.

Yes. The type of legal acts – law and administrative rule – chosen, considering the different levels of importance and technicality of the issues raised by Directive 2006/24/EC, and their respective nature, correspond to those usually chosen in Portugal for such kind of matters and for the transposition of European Union directives in general.

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 (see the reference made in art. 2 para 2. of the Directive that have also been legally defined in the national translation?**

Yes. Article 2 of Law 32/2008 establishes the relevant definitions for certain terms used therein.

The following definitions stated in Article 2 of Law 32/2008 are mere translations of the definitions included in the Directive: "data", "telephone service", "user ID", "cell ID" and "unsuccessful call attempt".

The definition of "user" was not included in Law 32/2008.

On the other hand, Law 32/2008 introduced two new definitions – "competent authorities" and "serious crime".

According to article 2, no. 2 of Law 32/2008, the definitions provided for in Law no. 67/98, of 26 October (which transposed Directive 95/46/CE) and Law 41/2004, of 18 August (which transposed Directive 2002/58/CE) shall also be deemed applicable for the purposes of Law 32/2008.

Law no. 67/98 (Directive 95/46/CE) includes the following definitions: "personal data", "processing of personal data", "personal data filing system", "controller", "processor", "recipient" and "data subject's consent" and "combination of data", all taken from Directive 95/46/CE.

Law 41/2004 (transposition of Directive 2002/58/CE) transposed the following definitions: "communication", "user", "traffic data", "location data", "value added service" and "call". The definition of "consent" stated in article 2 of Law 41/2004 (transposition of Directive 2002/58/CE) was not included in since its transposition was already assured by Law no. 67/98, of 26 October (transposition of Directive 95/46/CE).

A new definition – "subscriber" was included in Law 41/2004 (transposition of Directive 2002/58/CE). The definition of "electronic email" in Directive 2002/58/CE was not transposed by the Portuguese legislator.

Law 5/2004, of 10 February was responsible for the transposition of Directive 2001/21/EC. All the definitions stated by Directive 2001/21/EC were included in Law 5/2004, with the exception of "specific directives". The directives indicated in such definition were also transposed by Law 5/2004 (transposition of Directive 2001/21/EC, with the exception of Directive 97/66/CE, which was revoked by Directive 2002/58/CE, itself transposed by Law 41/2004 as referred above.

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 obligation fall short of those specified by the Directive? Do data on unsuccessful call attempts have to be retained?

According to Law 32/2008 (which transposed the Directive), the following categories of data have to be retained by the providers:

a) Data necessary to trace and identify the source of a communication:

(i) Concerning fixed network telephony and mobile telephony;

- the calling telephone number;
- the name and address of the subscriber or registered user;

(ii) Concerning Internet access, Internet email and Internet telephony:

- the user IDs allocated;

- the user ID and telephone number allocated to any communication entering the public telephone network;

- 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) Data necessary to trace and identify the destination of a communication:

(i) Concerning fixed network telephony and mobile telephony

- the numbers dialed and, in cases involving supplementary services such as call forwarding or call transfer, the number or numbers to which the call is routed;

- the name and address of the subscriber, or of the registered user.

(ii) Concerning Internet e-mail and Internet telephony

- the user ID or telephone number of the intended recipient of an Internet telephone call;

- the names and addresses of subscribers or registered users and user ID of the intended recipient of the communication.

c) Data necessary to identify the date, time and duration of a communication:

(i) Concerning fixed network telephony and mobile telephony

- the date and time of the start and end of the communication;

(ii) Concerning Internet access, Internet email and telephone Internet telephony

- 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;

- the date and time of the log-in and log-off of the Internet email service or telephone communications service through the Internet, based on a certain time zone;

d) Data necessary to identify the type of communication:

(i) Concerning fixed network telephony and mobile telephony

- the telephone service used;

(ii) Concerning Internet email and Internet telephony

- the Internet service used.

e) Data necessary to identify user's communication equipment or what purports to be their equipment:

(i) Concerning fixed network telephony

- the calling and called telephone numbers;

(ii) Concerning mobile telephony:

- the calling and called telephone numbers;
- the International Mobile Subscriber Identity (IMSI) of the calling party;
- the International Mobile Equipment Identity (IMEI) of the calling party);
- the IMSI of the called party;
- the IMEI of the called party;
- in the case of pre-paid anonymous services, the date and time of the initial activation of the service and cell ID from which the service was activated.

(iii) Concerning Internet access, Internet email and Internet telephony:

- the calling telephone number for dial-up access;
- the digital subscriber line (DSL) or other end point of the originator of the communication.

f) Data necessary to identify the location of the mobile communication equipment:

- the cell ID at the star of the communication;
- data identifying the geographic location of cells by reference to their cell ID during the period for which data communications data are retained.

The categories of data that must be retained under article 4 of Law 32/2008 (transposition of Directive 2006/24/EC) are exactly the same as those indicated in the Directive.

Yes. Telephony data and Internet data relating to unsuccessful call attempts must be retained where those data are generated or processed and stored by providers of publicly available electronic communications services or public communications networks, in the context of communications services, as provided in article 5 of Law 32/2008 (transposition of the Directive).

Data relating to unconnected calls cannot be retained.

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 of data revealing the content of electronic communications is prohibited according to article 1 of Law 32/2008 (transposition of the Directive).

Nonetheless, Law 41/2004 (transposition of Directive 2002/58/CE) allows the retention of data in certain cases and under certain conditions.

Additionally, the Code of Criminal Procedure (Decree-Law no. 78/87, 17 of February) establishes a restrictive recording and interception of communications policy.

Law no. 109/2009, 15 of December, commonly known as Cybercrime law (hereinafter, "Cybercrime law") (implementation of the Convention on Cybercrime under national legislation), also allows the seizure of email communications and records of communications of similar nature, as well as the interception of communications under similar circumstances as those stated in the Code of Criminal Procedure.

None of these cases, however, include data retention without cause (stockpiling).

Under Law 41/2004 (transposition of Directive 2002/58/CE):

1) Storage or other kinds of interception or surveillance of communications and the related traffic data by other than the users concerned is prohibited, except in case of prior and explicit consent of the latter (article 4).

2) Recordings of communications by and for public services intended to provide for emergency situations of any nature are permitted (article 4).

3) The processing of traffic data necessary for the purposes of subscriber billing and interconnection payments is permitted (article 6). Nonetheless, only the categories of data indicated in the applicable legal provision may be subject to processing and retention for a certain period of time.

4) Location data other than traffic data may only be processed after they are made anonymous (article 7).

5) Recording and processing of location data to bodies with legal competence to deal with emergency calls, with the purpose to respond to such call, is also allowed (article 7).

6) Processing of location data is consented if necessary for the provision of a value added service, provided the prior written consent of the data subject concerned has been obtained (article 7).

According to the Code of Criminal Procedure (Decree-Law no. 78/87, 17 of February):

1) the interception and recording of telephone conversations may be authorized by the competent judge if there is reason to believe that such procedure is indispensable for establishing the truth or otherwise if it is impossible or extremely difficult to obtain the relevant proof. Either way, such procedure may only be ordered by the judge in the course of the investigation of certain crimes indicated in the Code of Criminal Procedure. The interception and recording operations are authorized for a maximum period of 3 months, renewable under the same criteria as those applicable to its first admittance (article 187).

1) the judiciary authorities and criminal police authorities may obtain data about cellular location when the latter are necessary to eliminate any life endangering situation or serious physical integrity offense (article 252-A).

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

The retention and transmission of data pursuant to Law 32/2008 (transposition of the Directive) is exclusively mandated for the purposes of investigation, detection and prosecution of serious crimes by the competent authorities.

Furthermore, the transmission of data to competent authorities may only be ordered or authorized by reasoned Court order pursuant to the conditions stated in article 9 of Law 32/2008 (transposition of the Directive).

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 client, between a doctor and his/her patient, between a journalist and a whistle-blower)?

Law 32/2008 (which transposed the Directive) does not exclude such type of "sensitive data" from the obligation of retention pending over the providers. So, the answer would be no, there are not.

However, article 14 of the Cybercrime law states that the injunction for providing data or granting access to data is not applicable to obtain data from a computer system used within the legal profession, medical, banking and journalists' activity. According to this article, if during the proceedings it becomes necessary for the gathering of evidence in order to ascertain the truth, obtain certain and specific data in a given system, the judicial authority may order to the person (legal or individual) who has the control or availability of that data to communicate the latter or to allow access to them, under penalty of punishment for disobedience.

Additionally, the Code of Criminal Procedure forbids the interception and recording of conversations or communications between the defendant and its lawyer during the course of a criminal investigation, except if the judge has reasons to believe that they constitute the object or an element of the crime at stake (article 187).

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 distinction is based and the reasons therefor.**

The providers of publicly available electronic communications services or of public communications networks must retain the data concerned for a 1-year period from the date of the communication (article 5 of Law 32/2008 which carried out the transposition of the Directive).

No distinction is made according to the data categories involved.

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

According to article 2, number 1, paragraph f) and article 3, number 2 of Law 32/2008 (which transposed the Directive), a judge has to firstly order or authorize the transmission of the data to the competent authorities which are judicial authorities and criminal police authorities of the following bodies (hereinafter, the "competent authorities"):

Polícia Judiciária (Judicial Police);

Guarda Nacional Republicana (Republican National Guard);

Polícia de Segurança Pública (Public Security Police);

Polícia Judiciária Militar (Military Judicial Police);

Serviço de Estrangeiros e Fronteiras (Foreigners and Borders Department);

Polícia Marítima (Maritime Police).

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. 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 retention and transmission of data pursuant to Law 32/2008 (transposition of Directive 2006/24/EC) is exclusively mandated for the purposes of investigation, detection and prosecution of serious crimes by the competent authorities.

According to article 3, number 2, of Law 32/2008 (which transposed the Directive) in connection with the legal definition of "competent authorities" in article Law 32/2008, the retained data may be transmitted to the following authorities: Judicial Police, Republican National Guard, Public Security Police, Military Judicial Police, Foreigners and Borders Department and the Maritime Police.

Serious crimes are the following: terrorist crime, violent crime, highly organized crime, illegal restraint, kidnapping and hostage taking, cultural identity or personal integrity crimes, crimes against national security, counterfeiting currency and equivalent securities, and crimes covered by conventions on safety of air and sea navigation.

The retention of data pursuant to Law 32/2008 (transposition of the Directive) can only be used for the purposes indicated therein as abovementioned.

Law 32/2008 (transposition of the Directive) does not grant individuals the right to access the data retained directly.

In addition, the data subject cannot oppose himself to the retention and transmission of the respective data. The exercise of any access right by the data subject would have to be based on Law no. 67/98, of 26 October (transposition of Directive 95/46/CE) and exercised by means of the Portuguese Data Protection Agency (Comissão Nacional de Protecção de Dados), if deemed admissible by the latter.

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. suspected serious crime, specific risks to public safety)?**

There must be a reason to believe that the access by the competent authorities to the data retained is crucial to the truth-finding process, or that otherwise it would be impossible or very difficult to secure evidence in the scope of the investigation, detection, and prosecution of serious criminal offences (article 9 of Law 32/2008 which carried out the transposition of the Directive).

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?**

As referred above, under Law 32/2008 (transposition of Directive 2006/24/EC) individuals cannot have access to the data directly, only the competent authorities upon order or authorization of reasoned court order. The authorization of access may only be requested by the public prosecutor or by the competent criminal police authority.

There is no provision in Law 32/2008 (transposition of Directive 2006/24/EC) stating that the aggrieved party needs to be previously heard or otherwise involve him in the proceedings before the data is accessed. Therefore, our answer is no.

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?**

There is no provision in Law 32/2008 (transposition of the Directive) on this subject-matter. Therefore, our answer is no.

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

There is no provision in Law 32/2008 (transposition of the Directive) on this subject-matter. Therefore, our answer is no.

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

Recourse to the courts is always admissible according to the Portuguese law, even if later ineffective.

The Portuguese Data Protection Agency (Comissão Nacional de Protecção de Dados) is the authority incumbent for monitoring the compliance of the provisions of Law no. 32/2008 (transposition of the Directive) and Law no. 67/98, of 26 October (transposition of Directive 95/46/CE). Therefore, the most effective way to react to an unlawful data access or processing operation would be to file a complaint with the Portuguese Data Protection Agency.

Depending on the nature and seriousness of the infractions committed, the Portuguese Data Protection Agency would enforce the adequate penalties established by law (regulatory breaches) or forward the complaint to the prosecutor's office (criminal offences).

Infractions that are subject to criminal liability under the applicable law on personal data and privacy protection can be reported directly to the prosecutor's office by the aggrieved party.

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

No. The legal provisions on the issue of unlawful access to the data retained result from the obligation of the providers of public available electronic communications services or of public communications networks to take all appropriate technical and organisational measures to ensure that the data is secured and accessed by specially authorized personnel only (article 7 of Law no. 32/2008 which carried out the transposition of the Directive).

In practical terms, the protection against unauthorized access is assured by the way the software (the "SAPDOC") works.

Under article 13 of Law no. 32/2008 (transposition of Directive 2006/24/EC), the following law infringements are deemed as crimes and punished by imprisonment of up 2 years or a fine of up to 240 days and these penalties may be doubled under certain circumstances (please consult answers to question 30 below):

Failure to comply with any of the provisions on data protection or security indicated in article 7 of Law no. 32/2008;

Access to data by an unauthorized person (person that is not included in the list sent to the Portuguese Data Protection Agency by the providers subject to data retention duties identifying its personnel specially authorized to access the data retained).

Furthermore, Law no. 67/98, of 26 October (transposition of Directive 95/46/CE) states that any authorized person that gains unlawful access in general to personal data is subject to imprisonment for a maximum of 1 year or a fine of up to 120 days. These penalties are doubled if the unlawful access: (1) is achieved by means of violating technical security rules; (2) allows the infringer or third parties to know the personal data; or (3) provides the infringer or third parties with a benefit or material advantage (article 44).

Law 41/2004 (transposition of Directive 2002/58/CE) also sanctions the non-compliance with the security standards imposed by this diploma, in particular the non-compliance with the conditions stated therein concerning storage and access to data (article 14).

The purpose of such provisions is, we believe, more to dissuade possible infringers than to protect the data retained against unauthorized access in a particular way.

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

A judge must determine, of his own motion or upon request by any interested party, the destruction of data held by the "competent authorities", as soon as they are no longer required for their intended purpose.

Data are deemed to be no longer required for their intended purposes in the following cases: (1) definitive closure of criminal proceedings; (2) final acquittal; (3) final conviction; (4) proceedings that become time-barred; (5) amnesty (article 11 of Law no. 32/2008 which carried out the transposition of the Directive).

Dimension 2 (State – economy)

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

As referred above, all providers of publicly available electronic communications services or of public communications networks must retain the categories of data indicated in article 4 of Law no. 32/2008 which carried out the transposition of the Directive).

The most relevant providers would be the following: fixed telephone service providers, mobile telephone service providers, Internet Access service providers, broadband service providers, nomadic VoIP services.

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

No. Law no. 32/2008 (transposition of the Directive) is clear. All providers of publicly available electronic communications services or of public communications networks are subject to the retention of data obligation.

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

Law 41/2004 (transposition of Directive 2002/58/CE) does not indicate specifically the categories of data that have to be retained as Law no. 32/2008 (transposition of the Directive) was able to do, with the exception of the retention of traffic data necessary for the purposes of subscriber billing and interconnection payments, as follows (article 6 of Law 41/2004):

Number or identification, address and type of station of the subscriber;

Time and durations of the calls made;

Date of the call or service and called number.

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 unauthorized destruction, loss or alteration of the data)?

Yes. There are a number of legal obligations that need to be fulfilled by the providers of publicly available electronic communications services or of public communications networks in charge of the data retention (article 7 of Law no. 32/2008 which carried out the transposition of the Directive).

These obligations are mainly the following:

Ensure that the retained data are of the same quality and subject to the same security and protection as those in the network.

Take all appropriate technical and organisational measures to protect the data subject to retention duties against accidental or unlawful destruction, accidental loss or alteration, or unauthorized or unlawful storage, processing, access or disclosure. The data concerned (except for data on subscribers' name and address) must be blocked as from the moment they are retained, and shall only be unblocked in order to be provided to the "competent authorities".

Take all appropriate technical and organisational measures to ensure that the data subject to retention duties are accessed by specially authorized personnel only. For this purpose, the providers subject to the retention obligation are obligated to submit to the Portuguese Data Protection Agency (Comissão Nacional de Protecção de Dados), by electronic means only, the necessary elements to identify the personnel specially authorized to accessed the data retained.

Provide the data submitted to retention duties by means of an electronic communication, under the technical and security conditions imposed by Administrative Rule 469/2009, which must always meet the highest possible degree of codification and protection, according to the state of the art at the moment of transmission, including codification or encryption methods.

These obligations do not diminish the need of compliance with the principles and rules on quality and safeguard of confidentiality and security of data pursuant to Law no. 67/98 (transposition of Directive 95/46/CE) and Law 41/2004 (transposition of Directive 2002/58/CE).

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)?**

We were unable to collect any information in order to answer to this question. There is no official data on this.

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 right to reimbursement. The obligated parties are obliged to assume all costs and expenses necessary to assure their compliance with Law no. 32/2008 (which carried out the transposition of the Directive).

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 Administrative Rule 469/2009, upon receipt of a request for retained data by the judge through the SAPDOC, the provider shall immediately carry out the respective search, according to the chronological order in which requests are received or to the determined degree of urgency. As soon as the data search has been finalized, the provider must transfer the file that corresponds to the search result, through a secure and encrypted connection, authenticated with a a user name and password, and send the notification of reply file transfer trough the software, indicating the name of the transferred file (article 3 of Administrative Rule 469/2009).

The Instituto das Tecnologias de Informação na Justiça (ITIJ, I.P.) – the Institute of Information Technologies in Justice informed unofficially that there are rules governing the cooperation between the providers obligated to the data retention and such Institute in order to guarantee the efficiency of the software developed (the "SAPDOC"). Nonetheless, these are not statutory rules since they are of a contractual nature. For this reason, they were not made public and we were unable to gather particulars on their content.

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 obliged parties? Please describe the content of such rules.**

Yes. The obliged parties are subject to liability (administrative and criminal liability) in case of infringement of the provisions contained in Law no. 32/2008 (transposition of the Directive).

The following infringements are deemed as administrative offences and are punishable by penalties between 1.500 to 50.000 Euros or between 5.000 and 10.000 Euros, whether the infringer is respectively a natural person or a legal entity (article 12 of Law no. 32/2008 which carried out the transposition of the Directive):

Failure by entities subject to data retention duties to retain the necessary categories of data, as stated by law;

Non-compliance with the period of retention stated by law (one year);

Failure by entities subject to data retention duties to provided data to "competent authorities" which hold the necessary authorization, as stated by law;

Failure by entities subject to data retention duties to send to the Portuguese Data Protection Agency (Comissão Nacional de Protecção de Dados) the necessary elements to identify its personnel specially authorized to accessed the data retained, as stated by law.

The following law infringements are deemed as crimes and punished by imprisonment of up 2 years or a fine of up to 240 days (article 13 of Law no. 32/2008 which carried out the transposition of the Directive):

Failure to comply with any of the provisions on data protection or security indicated in article 7 of Law no. 32/2008;

Access to data by an unauthorized person (person that is not included in the list sent to the Portuguese Data Protection Agency by the providers subject to data retention duties identifying its personnel specially authorized to access the data retained).

The penalties above may be doubled under the following circumstances (non cumulative):

The crime was committed through infringement of safety technical standards;

The crime made the personal data available to the infringer or to third parties;

The crime has provided the infringer of third parties with material benefits or advantages.

In both cases - administrative offences and crimes – the mere attempt to infringe the law and an infringement situation attributable to negligent behaviour only are subject to liability as well.

Additionally, as mentioned above, these obligations do not diminish the need of compliance with the principles and rules on quality and safeguard of confidentiality and security of data pursuant to Law no. 67/98 (transposition of Directive 95/46/CE) and Law 41/2004 (transposition of Directive 2002/58/CE).

Law no. 67/98 (transposition of Directive 95/46/CE) is the only statute to rule on the civil liability of the infringer. Any person who has suffered damage as a result of an

unlawful processing operation (including unlawful retention and access under Law no. 32/2008) or any other act incompatible with legal provisions in the area of personal data protection is entitled to receive compensation from the controller for the damage (article 34 of Law no. 67/98 which carried out the transposition of Directive 95/46/CE).

Furthermore, Law 41/2004 (transposition of Directive 2002/58/CE) also sanctions the non-compliance with the security standards imposed by this diploma, in particular the non-compliance with the conditions stated therein concerning storage and access to data (article 14).

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 authorization of access to the data retained may only be requested by the public prosecutor or by the competent criminal police authority (article 9 of Law no. 32/2008 which carried out the transposition of the Directive).

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.

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?

There are no specific legal rules on this subject.

Nonetheless, for example, the providers subject to data retention duties are obliged to deliver the Portuguese Data Protection Agency (Comissão Nacional de Protecção de Dados) the following information concerning the preceding year:

The cases in which information was provided to the "competent authorities";

The time elapsed between the date on which the data were retained and the date on which the competent authority requested the transmission of the data; and

The cases where requests for data could not be met.

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

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 Portuguese authorities must cooperate with the competent foreign authorities for the purpose of criminal investigations or proceeding relating to computer systems or data, as well as the collection of evidence of a crime in electronic form, according to the rules on transfer of personal data contained in Law no. 67/98 (transposition of Directive 95/46/CE) (article 20 of Cybercrime law).

For purposes of international cooperation, and in order to provide immediate assistance for the purposes aforementioned, Polícia Judiciária (Judiciary Police) is obliged to maintain a structure that guarantees a point of contact available at all times, twenty-four hours a day, seven days a week (article 21 of Cybercrime law). The Judiciary Police must transmit to the Public Prosecution's Office any foreign requests regarding the access of data retained under Law no. 32/2008 (which carried out the transposition of the Directive). The Public Prosecution's Office then asks the judge to access and provide the relevant data, which is then sent back to the Judiciary Police and further forwarded to the foreign entity (Law no. 67/98 which carried out the transposition of Directive 95/46/CE and Administrative Rule 469/2009).

The foreign entities do not have the right to access directly to the data retained under (Law no. 32/2008 which carried out the transposition of the Directive).

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 independency 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 Portuguese Data Protection Agency (Comissão Nacional de Protecção de Dados) is the Portuguese authority endowed with the power to supervise and monitor compliance with the laws and regulations in the area of personal data protection, including the provisions of Law no. 32/2008 (transposition of the Directive) and Law 41/2004 (transposition of Directive 2002/58/CE).

The Portuguese Data Protection Agency (Comissão Nacional de Protecção de Dados) is an independent body with powers of authority that functions in close relationship with the Portuguese Parliament (article 22 of Law no. 67/98 which carried out the transposition of Directive 95/46/CE). Therefore, it has independence from the Portuguese Government and its Ministries.

The supervisory control exercised by the Portuguese Data Protection Agency (Comissão Nacional de Protecção de Dados) is comprehensive (it can incorporate a

legality and a technical advisability as well) as deemed necessary to pursue its duties and responsibilities pursuant to Law no. 67/98 (transposition of Directive 95/46/CE).

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 part thereof?

No. There are two decisions from the appeal courts (Tribunais da Relação) involving the applicability of Law no. 32/2008 (transposition of the Directive) but none of them raise any questions or concerns about the legality of Law no. 32/2008.

If so, please answer to the following questions:

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

Please see answer to question 36 above.

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

Please see answer to question 36 above.

c) Please describe firefly the outcome of concluded proceedings and the essential grounds of the rulings issues. 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 difference to previous case-law that deals the legitimacy of other collections of personal data?

Please see answer to question 36 above.

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 in which your Member State is/was involved (the indication of the case number is sufficient)?

We are not aware of any lawsuit with this scope.

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

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

We were unable to access to any information that might be able us to provide reliable information on the subject.

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

Storage outside Portugal is not barred by the Portuguese law and, therefore, it would be admissible according to Law no. 67/98 (transposition of Directive 95/46/CE). However, being the providers the data controllers they would have to comply with the legal rules concerning the security and confidentiality of the information, transfer of personal data to EU countries and third countries as well as data processing carried out by a processor on behalf and under the instructions of the data controller (articles 18 to 20 of Law no. 67/98 which carried out the transposition of Directive 95/46/CE).

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

a) No data are retained beyond what is permitted?

We are not aware of the technical and organizational measures that ensure in practical terms that no data are retained beyond what it is permitted. The information we were able to collect are only those resulting from the legal obligations of the service providers and the legal requirements under which a judge may order the destruction of the data.

The service providers are obliged to destroy the data at the end of the period of retention (1 year), except those that have been preserved by Court order, and to further destroy such preserved data upon order of the judge (article 7 of Law no. 32/2008 which carried out the transposition of the Directive).

The concerned judge determines, of his own motion or upon request by any interested party, the destruction of data held by the "competent authorities" and by the service providers, as soon as they are no longer required for their intended purpose. Data are deemed to be no longer required for their intended purposes in the following cases: (1) definitive closure of criminal proceedings; (2) final acquittal; (3) final conviction; (4) proceedings that become time-barred; (5) amnesty (article 11 of Law no. 32/2008 which carried out the transposition of Directive 2006/24/EC).

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)?

As previously refereed, the transmission of data to the "competent authorities" (State bodies) can only take place upon order or authorization by the concerned judge (article 13 of Law no. 32/2008 which carried out the transposition of the Directive).

The relevant data must be provided by the services providers by electronic means, under the technical conditions laid down in Administrative Rule 469/2009. The electronic communication must be processed on the basis of a specific software (called "SAPDOC"), through which the judge sends out the data request and the providers notify the transmission of the file that corresponds to the search result (the "reply files"). After receiving the request, the judge must decrypt it and make it available to the "competent authority" (articles 2 to 4-A of Administrative Rule 469/2009).

Therefore, the "competent authorities" cannot gain direct access to the retained data.

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

The providers are bound to prepare records on the data retrieved upon resonated Court order and send them to the Portuguese Data Protection Agency (Comissão Nacional de Protecção de Dados) (article 9 of Law no. 32/2008 which carried out the transposition of the Directive).

The security measures established by Administrative Rule 469/2009 were designed to restrict the number of persons who may have access to the retained data and therefore restrict as much as possible the use of the retained data for any unauthorized purposed.

All retained data is encrypted before being sent by the providers to the concerned judge. The judge order authorizing the data transmission and the reply file of the provider must bear an electronic signature.

There must be kept an electronic record of data requests (with indication of who sent the request and the time and date when it was sent) and an electronic record of all accesses to reply files (with indication of who requested the access and the respective time and date).

The reply files are stored in separate folders (one for each provider) as to avoid the interconnection of data).

The data contained in the reply file (which is encrypted) may only be viewed electronically through the SAPDOC. The SAPDOC is subject to security audits.

The concerned judge may only access the SAPDOC by introducing his user name and password (article 5 of Administrative Rule 469/2009).

The security measures provided for in Law no. 32/2008 (transposition of the Directive) and Law no. 67/98 (transposition of Directive 95/46/CE) are also applicable and therefore used to avoid and dissuade unlawful use of the data.

d) data are protected against unauthorized 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 principles along with secure authentication, local/decentralized storage etc)? Please describe the measures taken both by the party retaining the data and by the party accessing them.

Please see answers given about the questions included in paragraph c) of this question.

Additionally, the data subject to the retention obligation (except for data on subscribers' name and address) must be blocked from the moment they are retained and shall only be unblocked to be provided to the "competent authorities" through the concerned judge (article 7 of of Law no. 32/2008 which carried out the transposition of the Directive).

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

We are not aware of the technical and organizational measures that ensure in practical terms that the data are destroyed safely and immediately upon expiry of the retention period provided by law.

But under Law no. 32/2008 (transposition of the Directive) failure to comply with the obligation to destroy the data upon expiry of the retention period or its order of destruction by the concerned judge is a crime punished by imprisonment of up to two years or a fine up to 240 days. These penalties shall be doubled where the crime (1) was committed through infringement of safety technical standards; or (2) has made personal data available to the infringer or third parties; or (3) has provided the infringer or third parties with material benefits or advantages.

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)?

No. There is no legal obligation to notify the aggrieved parties. However, as previously referred to, any interested party may request the concerned judge the destruction of data held by the "competent authorities", as soon as they are no longer required for their intended purpose. Data are deemed to be no longer required for their intended purposes in the following cases: (1) definitive closure of criminal proceedings; (2) final acquittal; (3) final conviction; (4) proceedings that become time-barred; (5) amnesty (article 11 of Law no. 32/2008 which carried out the transposition of the Directive).

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

We are not aware of the technical and organizational measures that ensure in practical terms that the "sensitive data" referred to in question 12 are not

retained or transmitted. The applicable legal provisions do not dwell on the subject.

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)?

Please see answer to question 35. Any control is exercised by the Portuguese Data Protection Agency (Comissão Nacional de Protecção de Dados).

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?

We are unable to provide particulars on the technical standards applied by the providers concerning the data retention.

As regards to the transmission of the retained data by the providers to the concerned judge, the latter must be made by means of an electronic communication under the technical and security conditions set out in Administrative Rule 469/2009.

Interoperability of the systems of the providers and "competent authorities" was not the technical choice of the Portuguese Government. The electronic communication above mentioned must be processed on the basis of a specific software (the "SAPDOC"), through which the judge sends out the data request and the providers notify the transmission of the file that corresponds to the search result (the "reply files"). Please see answer to paragraph c) of question 40.

We do not have additional information on this subject.

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

The judge that ordered or authorized the transmission of data retained by the providers communicates the decision using the software known as SPADOC (System of Access to or Request of Data from Communication Operators) specifically made available for this purpose.

The communication is carried out by filling in the electronic form available at SAPDOC, which includes an order of the judge, based on a substantiated order included in the proceedings file only, which specifically authorizes the transmission of data.

The form aforementioned must include: (a) all information necessary to identify the applicant, the proceedings file and the court or organizational unit where it takes place, which must be filled in automatically where technically possible; (b) the order of the judge, drew up through the validation of an electronic mode; (c) data to be

transmitted by the providers; and, (4) the determined degree of urgency, where appropriate. After the form is fully filled in, the SPADOC shall automatically generate, based on data entered, a PDF bearing the digital signature of the judge. The inclusion of the electronic signature shall automatically and electronically trigger the submission to requested parties of structured data in PDF format.

Upon receipt of a request for data, the provider must immediately carry out the respective search, according to the chronological order in which requests are received or to the determined degree of urgency.

As soon as the data search has been finalized, the provider must: (a) transfer the file that corresponds to the search results through a secure and encrypted connection, authenticated with a user name and password; (b) send the notification of the reply file transfer through the SAPDOC, indicating the name of the transferred file.

The SAPDOC notifies the provider that the reply file has been successfully received and stores.

After receiving the request, the judge must decrypt it and make it available to the competent judge or agent, where possible by electronic means.

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

The SPADOC cannot be used directly by any foreign entity.

Therefore, in practical terms foreign entity would have to present a request to the Portuguese "competent authority" (Judiciary Police in this case), which would then forward such request to a judge authorized to use the SAPDOC.

The judge with access to the SAPDOC would have to make a request to the service providers regarding the concerned data. As soon as the judge received the data, which would be encrypted, he would send it to the Portuguese "competent authority". Only then it would be delivered to the foreign entity by the Portuguese "competent authority".

As far as we know, the information would be provided in Portuguese.

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, labor unions as well as other professional organizations 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).

There is not a public debate on this issue. We believe the public in general, and the end consumer as well, is not aware that their personal data are retained by the service providers under Law no. 32/2008 (transposition of the Directive) and its implications in terms of protection of privacy and personal data.

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

There are several cases where the data controllers are obligated to retain personal data but all those are related to a specific reason: invoice purposes, compliance to legal obligations of the data controller (e.g. tax duties), consumer protection, etc.

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

The Portuguese Data Protection Agency (Comissão Nacional de Protecção de Dados) should provide the Commission of the European Communities with annual statistics on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or a public communications network using the information indicated in the answer to question 33 (article 16 of Law no. 32/2008 which carried out the transposition of the Directive). However, we were unable to obtain such information from the Portuguese Data Protection Agency (Comissão Nacional de Protecção de Dados).

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?

We are not aware of the existence of such information.

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 no public discussion on the matter. The categories of data to be retained are exactly those contemplated in the Directive, so it is unlikely any diminishment or increase of such categories.

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 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.)? 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) law – considered as telecommunications content? Is it legal under national (constitutional) law to retain this content without a specific reason?

The fundamental rights protecting privacy, personal data and the secrecy of telecommunications according to the Portuguese Constitution are the following: right to the inviolability of home and correspondence and right to privacy and, consequently, of protection of personal data, pursuant to articles 34 and 35 of the Portuguese Constitution.

With regard to the right of inviolability of one's home and correspondence, the secrecy of means of private communication is deemed inviolable. Therefore, public authorities are prohibited from interfering in any way with telecommunications or other means of communication, save in such cases as the law may provide for in relation to criminal proceedings.

According to the constitutional right to privacy and personal data protection, every citizen possesses the right to access to all computerized that that concerns him, to require that they be corrected and updated, and to be informed of the purpose for which they are intended, all as laid down by law. Computers must not be used to treat data concerning private life, save with the express consent of the data subject, with authorization provided for by law and with guarantees of non-discrimination. Third-party access to personal data is prohibited, save in exceptional cases provided for by law.

We do not believe that other fundamental rights other than those aforementioned may be substantially affected since the retention obligation does not include the content of any conversations or written communications of the data subject. At least not until a criminal procedure is initiated.

The Portuguese Constitution does not establish what the legislator must consider as telecommunications content when legislating on the matter.

It is illegal to retain the content of any private communication without a specific reason indicated by law as justifiable to challenge the fundamental rights above indicated.

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 Portuguese Constitution states that the national law may only restrict rights, freedoms and guarantees in cases expressly provided for in the Constitution, and such restrictions must be limited to those needed to safeguard other rights and interests protected by the Constitution.

Therefore, the restrictions imposed by Law no. 32/2008 (transposition of the Directive) are considered acceptable considering the interests at stake, i.e. the protection of other constitutional rights which, under certain circumstances, should prevail: e.g. access to effective judicial protection, right to life and personal integrity, right to security, etc.

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, it has not.

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

When approving legal acts, the Portuguese legislator (the Portuguese Parliament or the Government) must balance the fundamental rights that will be restricted considering the fundamental rights that will be protected in result therefrom. In any case, as referred above, any restrictions must be limited to those needed to safeguard other rights and interests protected by the Constitution.

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)?

No, it does not.

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?

Until this point the subject has not earned the attention of the scholars and media.

It would be possible to argue that the retention obligation goes beyond what the Constitution admits in terms of restriction of to one's right to privacy as a fundamental right.

Under article 34 of the Constitution, the individual's home and the privacy of his correspondence and other means of private communications are inviolable. Consequently, any interference by public authority with correspondence or telecommunications is, by principle, prohibited. The only exception to such absolute right is the situations provided by law in connection with criminal procedures. But the data retention obligation is due by the providers prior to the existence of any criminal procedure against the data subjects. The data retention obligation is a precautionary measure, not an exceptional measure to ascertain the truth reading a specific criminal action.

Anyone using a telecommunications service available in the Portuguese market today is subject to having his data retained under Law no. 32/2008 (transposition of the Directive) by the concerned services providers, during the period of one year, for the hypothetical event that such data may be needed in a future criminal procedure involving the data subject. For that reason, there will be a significant amount of personal data retained by private actors without any connection to a certain and determined criminal procedure.

But, on the other hand, article 35 of the Constitution also states that computerized storage can be used for information concerning a person's private life when there is an authorization provided for under the law with guarantees of non-discrimination.

There is a clear margin for legal arguments and discussions.

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)?

Under Law no. 32/2008 (transposition of the Directive) the only private actors involved in the process of the data retention for the purpose of investigation, detection and prosecution of serious crimes by the competent authorities are the service providers. And their intervention is limited to the obligation to retain the data.

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

No. The Constitution does not dwell on this subject. Therefore, upon the silence of the constitutional and national law, the reimbursement is not due.

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 the Portuguese Constitution, the rules set out in duly ratified or approved international agreements by Portugal come into force in the Portuguese internal law once they have been officially published in the Portuguese Official Gazette (Diário da República), and they remain valid and enforceable as long as they are internationally binding on the Portuguese State.

Most legal writers believe that the Portuguese Constitution endorses the automatic reception clause (or self-executing clause). Therefore, if the concerned international treaty complies with the aforementioned requirements, it comes into force in Portuguese internal law.

Portugal ratified the European Convention on Human Rights (ECHR) on October 13, 1978 (Law 65/78) and currently in force.

The majority of the Portuguese legal scholars advocate that treaties are graded below the Constitution but, nonetheless, supersede national legislation.

The Portuguese Constitution has far-reaching provisions on fundamental rights and guarantees. Therefore, petitions to the Portuguese courts are not common due to the extensive protection provided by the Constitution. In case of clash between both texts, the rights protected under the Constitution would prevail.

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?

The provisions of the treaties of the European Union and the rules issues by its institutions in the exercise of their respective competences are applicable in the Portuguese internal law in accordance with the Union law.

The principle of the direct effect of Directives, as developed by the ECJ, is accepted by the Portuguese doctrine and recognized by the court (Supreme Court's ruling of 01.10.1996, Ca96A204)

The obligations stated by the concerned Directive must be precise, clear and unconditional and not call for additional measures, either national or Community in order to supersede the national legislation in force.

If the concerned Directive grants the State Member a certain margin of discretion, however minimal, regarding the implementation of the EU provision in question, then the Directive is denied of direct effect.

The transposition of Directives is carried out by the Portuguese Parliament or by the Government depending of its subject-matter. According to the Portuguese Constitution, the Portuguese Parliament possesses the exclusive responsibility to legislate about certain matters and, therefore, any Directives following under the scope of such exclusive responsibility must be transposed by a legal act approved by the Portuguese Parliament.

As regards to other subject matters stated in the Portuguese Constitution, the Portuguese Parliament has a partially exclusive responsibility to legislate, meaning that, unless it also authorizes the Government to do so, the Portuguese Parliament also possesses the exclusive responsibility to legislate about those matters.

All the remaining issues contained in the European Directives, i.e. those that do not belong, either partially or exclusively, to the legislative power of the Portuguese Parliament, are the responsibility of the Government.

In several situations the Portuguese legislation requires the prior hearing of another entity or authority at the time the Parliament or the Government is working on the diploma that will carry out the transposition of a Directive.

For example, according to Law no. 67/98 (transposition of Directive 95/46/CE), the Portuguese Data Protection Agency (Comissão Nacional de Protecção de Dados) must be consulted on any legal provisions and on legal instruments in preparation in Community or international institutions relating to the processing of personal data.

In any case, however, the responsibility for the transposition of Directives falls upon the legislative entities: the Portuguese Parliament and Government.

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?

Pursuant to article 8 of the Portuguese Constitution, The provisions of the treaties of the European Union and the rules issues by its institutions in the exercise of their respective responsibilities are applicable in the Portuguese internal law in accordance with the Union law and with respect for the fundamental principles of a democratic state based on the rule of law.

Any transfer must be limited to the respect for and the guarantee of the effective implementation of fundamental rights and freedoms.

Furthermore, according to the Portuguese Constitution, Portugal may enter into agreements for the exercise, jointly in cooperation or by the EU institutions, of the powers needed to construct and deepen the European Union.

However, this possibility is also subject to reciprocity and to the respect for the fundamental principles of a democratic state based on the rule of law and the principle of subsidiarity, in order to achieve the economic, social and territorial

cohesion of an area of freedom, security and justice and the definition and implementation of a common external security and defense policy.

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?

As referred above, the Portuguese Data Protection Agency (Comissão Nacional de Protecção de Dados) is the Portuguese authority endowed with the power to supervise and monitor compliance with the laws and regulations in the area of personal data protection, with strict respect for human rights and the fundamental freedoms and guarantees enshrined in the Portuguese Constitution and the law.

The Portuguese Data Protection Agency (Comissão Nacional de Protecção de Dados) must be consulted on any legal provisions and on legal instruments in preparation in Community or international institutions relating to the processing of personal data. It is an independent body with powers of authority operating within the Portuguese Parliament, which possesses exclusive responsibility to legislate on any matters involving rights, freedoms and guarantees, including any restrictions applicable to the latter.

The Portuguese Data Protection Agency (Comissão Nacional de Protecção de Dados) exercises its authority throughout the Portuguese territory regardless the national law applicable to the data operation in question.

Therefore, the Portuguese Parliament and the Portuguese Data Protection Agency are the main players in terms of data protection regulations and proceedings.

Because Law 32/2008 (transposition of the Directive) determined that data on categories provided for in article 4 thereof (traffic and location data on natural persons and legal entities, and related data necessary to identify the subscriber or registered user) should be provided "by electronic means, under the technical and security conditions set out in a joint administrative rule of members of the Government for internal administration, justice and communications. Administrative Rule 469/2009 laid down those conditions.

In accordance with the framework established by Administrative Rule 469/2009, the communications operators adopted the necessary preparation with the Ministry of Justice, having the Instituto das Tecnologias de Informação na Justiça (ITIJ, I.P.) – the Institute of Information Technologies in Justice – ensured the development of the software the creation of which has been determined (the "SAPDOC"). But the intervention of the Ministry of Justice and its Institute of Information Technologies in Justice is mostly on a technological level, ensuring the functionality and usability of the software in use (the SAPDOC) for the data transmission.

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

The national (constitutional) law does not govern the transmission of retained personal data to other countries.

The only existing legal provisions on this subject are those resulting from the transposition into the Portuguese national order of Directive 95/46/CE which was achieved by the approval of Law no. 67/98, a ordinary law, not a constitutional law.

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?

Considering the aforementioned, we believe the Portuguese legal framework on data retention to be quite balanced.

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

Portugal

Carlos de Almeida Sampaio/Inês Sá

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*?

No. There is no specific provision in the Portuguese Constitution stating that one has the right to communicate anonymously.

Nonetheless, this right may be claimed under the following provisions of the Portuguese Constitution:

a) Article 26 on *Other personal rights*

1. Everyone shall possess the right to a personal identity, to the development of their personality, to civil capacity, to citizenship, to a good name and reputation, to their likeness, to speak out, ***to protect the privacy of their personal and family life****, and to legal protection against any form of discrimination.*

2. The law shall lay down effective guarantees against the procurement and misuse of information concerning persons and families and its use contrary to human dignity. The law shall guarantee the personal dignity and genetic identity of the human person, particularly in the creation, development and use of technologies and in scientific experimentation.

3. Deprivation of citizenship and restrictions on civil capacity may only occur in such cases and under such terms as may be provided for by law, and shall not be based on political motives.

b) Article 34 on the *Inviolability of home and correspondence*

4. Personal homes and the secrecy of correspondence and other means of private communication shall be inviolable.

5. *Entry into a citizen's home may only be ordered by the competent judicial authority and then only in such cases and in compliance with such forms as may be laid down by law.*

6. *No one shall enter any person's home at night without his consent, save in situations of flagrante delicto, or with judicial authorisation in cases of especially violent or highly organised crime, including terrorism and trafficking in persons, arms or narcotics, as laid down by law.*

7. *The public authorities shall be prohibited from interfering in any way with correspondence, telecommunications or other means of communication, save in such cases as the law may provide for in relation to criminal proceedings.*

Please bear in mind that these rights may be restricted if, under specific circumstances clearly provided by law, they are considered to be less important than other constitutionally protected rights (e.g. criminal investigation procedures of certain crimes).

Therefore, they are not considered to be absolute, unquestionable and undisputable rights, which mean they can be sacrificed in exceptional cases.

2. Please illustrate in detail any amendments to current data retention legislation that have been adopted since your answers to the last questionnaire, or 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 current data retention legislation since our last report was submitted.

Therefore, the current legal regime on data retention remains the following:

• Law 32/2008, of 17 July (hereinafter, "Law 32/2008"), transposed to the Portuguese legal order Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 (hereinafter, "Directive 2006/24/EC), on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks. It has suffered no amendments since our first report on data retention.

• Administrative Rule 694/2010, of 16 August (hereinafter "Administrative Rule 694/2010") laid down the technical and security conditions under which electronic communications for the transmission of traffic and location data on natural persons and legal entities must operate, and also of related data necessary to identify the

subscriber or registered user, pursuant to Law 32/2008. Its text has not been altered in any way since our first report.

During the last parliamentary term, there were rumours about the alteration of the current legal framework on data retention.

But the Portuguese Government resigned in the meantime, a new Government took office and FMI intervened in Portugal.

The current parliament and executive cabinet are extremely preoccupied with fulfilling Troika's expectations about the drastic reduction of the State's budget deficit.

Therefore, lawmaking and parliamentary works has been, for some time, now solely focused on the austerity measures and other cost reduction measures.

Pursuant to article 23, paragraph a) of the Portuguese Data Protection Law as approved by Law 67/98 dated of 26 October (hereinafter, "Data Protection Law"), the Portuguese Data Protection Authority (*Comissão Nacional de Protecção de Dados*) is responsible for issuing opinions on national legal provisions, and on legal instruments being prepared by the EU or international institutions, relating to the processing of personal data.

Therefore, any draft legislation involving personal data should have been submitted to this authority for evaluation during these latest months.

The Portuguese Data Protection Authority publishes in its website all legal opinions delivered to the Portuguese Parliament or Government.

But according to the information currently available on its on-line database, no legal advice has been issued on data retention by this authority since our first report, so we may only suspect that no progress has been by the current parliament to alter the current legal framework on data protection.

We believe this to be a direct result of the country's economic situation. The political and decision making environment is focused in the correction of the country's excessive deficit. Therefore, in virtue of current economic and political context, data retention issues are not a priority.

The issues that have been publicly discussed since the beginning of 2011 are mainly related with the current adverse economic context as mentioned above.

Data retention, privacy and data protection are not in Portugal's agenda at this point, unless it becomes necessary to do so in order to comply with secondary community legislation.

With regard to the last question, the issue has been thought by the Portuguese lawmaker, even if in a cursory manner.

Law 109/2009 dated of 15 of December, commonly known as Cybercrime Law (hereinafter, "Cybercrime Law"), adapted into national law the Convention on Cybercrime of the Council of Europe.

The procedural provisions contained in the Cybercrime Law, which are applicable to proceedings on criminal offences where the collection of electronic evidence is required, shall be without prejudice of the obligation to retain data laid down in Law 32/2008 aforementioned [according to article 11 (2) of Cybercrime Law].

At this point, the data retention obligation needs to be carried out without prejudice of a possible injunction to submit or provide access to computerized data under the Cybercrime Law.

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?**

On the one hand, if the collection of evidence necessary to uncover the truth requires that specified computer data is obtained (including traffic data that has been stored by means of a computer system), and in particular where there are grounds to believe that the computer data are particularly vulnerable to loss, modification or unavailability, the competent judicial authority shall order whoever holds or controls such data to preserve the data, including the service provider.

This data preservation order must indicate the period of time over which data must be preserved, up to three months.

In compliance with such preservation order, whoever holds or controls such data, namely the service provider, shall promptly preserve the data, protecting and maintaining its integrity for the established period of time, to enable the competent judicial authority to obtain it, being subject to ensure that the undertaking of such procedures is kept confidential.

The competent judicial authority may order the renewal of the measure up to a maximum limit of one year.

On the other hand, in order to ensure the preservation of traffic data related to a specific communication, regardless of whether one or more service providers were involved in the transmission of that communication, the service provider which was ordered to preserve data shall indicate to the judicial authority or to criminal police bodies, as soon as this information is available to it, other service providers through which the communication was made, in order to identify the service providers and the path through which the communication was transmitted.

If an injunction to submit or provide access to data has been issued, whoever holds or controls the data under consideration is obliged to provided it to the competent judicial authority or provide access to the computer system where such data are stored, on pain of criminal punishment for disobedience.

The obligations referred to above are included in the Cybercrime Law abovementioned, which is applicable to the following proceedings on criminal offences:

a) Those specifically indicated in the Cybercrime Law;

b) Those committed by means of a computer system;

c) Those where the collection of electronic evidence is required.

Also, there is a general duty to collaborate with the administration of justice and to respond to an order given by a judiciary authority, provided such order is legitimate pursuant to the applicable law. According to article 348 of the Portuguese Penal Code, whoever fails to abide to a legitimate order issued by court is punished with a penalty of up two years of imprisonment or payment of a fine of up to 240 days. The judicial order is legitimate if it is in accordance with the law as aforementioned.

Other than this, the offended party in a criminal proceeding that decides to appear as a (joint) plaintiff is required to collaborate with the Public Prosecutions Office. The plaintiff is entitled to intervene in the investigation, either by providing and/or demanding evidences (article 69 of the Criminal Procedure Code). But no victim or affected party is legally required to become a plaintiff in a proceeding on a criminal offence, if they do not want to.

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?**

The accused in a criminal proceeding is not obliged to provide answers to the questions addressed to him by any entity regarding the facts he is accused of, nor is he obliged to provide information about the content of the statements he has given about such facts (article 61 of the Criminal Procedure Code).

According to article 132 of the Criminal Procedure Code, a witness is not bound to give answers to questions when she claims they might result in self-incrimination.

At the same time, individuals that have a close personal connection to the accused have the right to refuse to testify as witnesses under article 134 of the same code: (a) descending and ascending relatives of the accused, his brothers and sisters, spouse, kin up to the second degree, his adopters and those adopted by him; and (b) anyone who has been married to the accused or has lived with him under analogous terms to marriage with regard to facts that have occurred during marriage or cohabitation period.

Article 135 of the Criminal Procedure Code establishes the existence of statutory obligations of secrecy upon certain professions.

The ministers of religion or religious confession, lawyers, physicians, journalists, members of credit institutions and other people to whom the law allows, or imposes on, professional secrecy may be excused from testifying in facts covered by the mentioned secrecy.

However, this is not an undisputed neither an absolute right.

If there are well grounded doubts on the excuse's legitimacy, the authority before which the professional secrecy has been argued may proceed with the necessary investigations. If after they take place, the authority decides that the excuse is illegitimate, the court is entitled to order giving of evidence.

The court immediately above to the one before which the obligation of professional secrecy was brought up, or in the event the issue was arisen before the Supreme Court, the plenary of criminal chambers may decide in favor of the giving of evidence with breach of professional secrecy, whenever it is proved that this is justifiable according to the principle of the prevailing interest preponderance, including, without limitation, crucial need of the giving of evidence to the truth-finding process, the seriousness of the crime committed and the need to protect legal assets and/or individual rights.

Searches to lawyers or doctors' offices (premises related to activities involving privileged information) can take place under article 180 of the Criminal Procedure Code.

However, documents covered by the obligation of professional secrecy of lawyers and doctors cannot be seized provided that they are not the object or an element of the crime. Any proof obtained in violation of this restriction is considered to be null and void and may not be used in a court of law.

Interception and recording of conversations and communications between the accused and his lawyer are not permitted, except if the judge has reasonable grounds to believe that such conversations and communications are the object or an element of the crime (article 187 of the Criminal Procedure Code).

The injunction to submit or provide access to data pursuant to article 14 of the Cybercrime Law may not be used as regards to computer systems used in legal, medical and bank practices, as well as by journalists.

Also, this same injunction cannot be addressed to the suspect or defendant in a proceeding on criminal offence.

Seizures related to computer systems used for legal, medical and bank practices are possible under article 16 of the Cybercrime Law. But they need to comply with the rules and formalities provided for in the Criminal Procedure Code, duly adapted.

In theory, there may exist situations where the data retained under Law 32/2008 (transposition of Directive 2006/24/EC) would not have been made known to the judicial authority according to the remaining rules of the criminal procedure.

But the majority of legal provisions existing in the Portuguese legal framework let us understand that these are not absolute rights and they can be overridden in certain circumstances.

As we mentioned before, even the duty of professional secrecy may be pushed way by a court order.

In addition to this, the data retained under Law 32/2008 cannot reveal the content of electronic communications. The categories of data retained under Law 32/2008 serve to determine the identity of the user and particulars about a certain electronic communication (date, time, destination, etc.). Contents of conversations cannot be processed nor retained.

So, it seems that the main problem with Law 32/2008 is not the retention of data about the accused in a proceeding of criminal offence.

What is more worrying in terms of personal data and protection of privacy is that all individuals see their personal data retained for a whole year under Law 32/2008, whether or not they are involved in a proceeding on criminal offence.

And just so that, in case such uncertain event is to occur, the retained data might be useful for the investigation, detection and prosecution of serious crimes (terrorist crime, violent crime, highly organized crime, illegal restraint, kidnapping and hostage-taking, cultural identity or personal integrity crimes, crimes against national security, counterfeiting currency or equivalent securities, and crimes covered by conventions on safety of air or sea navigation).

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?**

   We found no information publicly available on how this is carried out.

   We can only assume that this information gets the same treatment as any information included in an proceeding on criminal offence.

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.

The *Instituto das Tecnologias de Informação na Justiça* (ITIJ, I.P.) – the Institute of Information Technologies in Justice is not required to keep a data base on this matter.

Providers of publicly available electronic communications services or of public communications networks (hereinafter "providers") are required to deliver to the Portuguese Data Protection Agency until 1 March every year, the following information, concerning the preceding year:

a) The cases in which information was provided to the competent authorities;

b) The time elapsed between the date on which the data were retained and the date on which the competent authority requested the transmission of the data; and

c) The cases where requests for data could not be met.

Therefore, until March 2011 this information should have been produced, at least in theory, by the providers.

However, we are not aware if the information has been delivered to the Portuguese Data Protection Agency as there is no official information available on the matter.

Unfortunately, we may not provide useful information as required.

B. Country-specific questions

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

We are sure that the unconstitutionality of Law 32/2008 will be argued at some point before the courts of first instance.

However, in our opinion, its constitutionality may be defended as whole even if we argue that the Portuguese Constitution is above secondary community legislation like Directive 2006/24/EC.

First of all, there are no other means available to obtain access to the categories of data to be retained under Law 32/2008.

Truth be told that, although article 14 of the Cybercrime Law foresees the possibility of an injunction for the delivery or access to data held by service providers (defined as being public or private entity that provides to users of its service the ability to communicate by means of a computer system, as well as any other entity that processes or stores computer data on behalf of such communication service or users of such service), such data may not addressed to a suspect or defendant in those proceedings.

This injunction may also not be used as regards computer systems used in legal, medical and bank practices, as well as by journalists and the regime governing professional, staff and State secret information, provided for in article 182 of the Criminal Procedure Code, shall apply hereto, duly adapted.

On the contrary, data transmission to the competent authorities under Law 32/2008 may concern the suspect or defendant as well as the person who acts as an intermediary, where there are clear grounds for believing that such person receives or transmits messages to or from the suspect or defendant. The investigating authorities have then access to data that could not be obtained otherwise.

So, when we question ourselves if there are other means available to obtain the same result, the answer would be no (principle of necessity). Especially if we take into consideration that this information will be available for an entire year in case they are need during such period of time.

Secondly, we are required to consider whether or not data retention is in fact effective as regards to investigation, detection and prosecution of serious crime.

The *occasio legis* of Law 32/2008 (and of Directive 2006/24/EC), which was closely linked to the terrorist attacks in Madrid, was determinant for its approval and cannot be ignored. At the time, it seemed a small, controlled price to pay for an effective prevention against terrorism (principle of adequacy).

However, it is important to consider how long will last this *occasio legis* and for how long will the cost-benefit relationship be arguable in favour of data retention. This may change the current legal scenario on data retention and its legitimacy.

Finally, the bigger the intervention restraining a fundamental right – such as the right to privacy under data retention duty –, the higher intensity of the fundamental right we should be trying to protect.

In practical terms, some fundamental rights are, under certain specific circumstances, more worth than others (principle of proportionality *strict sensu*).

This is where we believe the main fragility of Law 32/2008 is located, particularly when analysing the criminal offences that may be included in the definition of "serious crimes" used by Law 32/2008 in result of the poor legal technique employed in this definition.

There are a considerable number of criminal offences that should not, in our opinion, yield before the right to privacy and that were (inadvertently?) included in the definition of "serious crimes" used to justify the need to retain data under Law 32/2008.

Apparently, the Portuguese lawmaker considered that the "crimes against national security" and "crimes regarding counterfeiting currency or equivalent securities" were violating one's constitutional right to safety (article 27) and, therefore, could justify data retention under Law 32/2008. It is our belief that the right to privacy is not susceptible of being bent in result of criminal offences contained in those parts of the Portuguese Penal Code.

But, as a whole, especially when considering fight against terrorism, where one's right to life and right to physical integrity may be directly affected, the data retention legal system should be deemed in accordance with the Portuguese Constitution.

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

   According to some Portuguese legal doctrine, yes.

   Article 34 of the Portuguese Constitution firstly protects the confidentiality of the contents of one's correspondence and as well as information transmitted through other means of communication.

   However, that protection should be extended to the circumstances under which the communications were made.

   Therefore, data concerning the means of communication that were used, the date, duration and location of that same use and users' identity should also be considered to be protected under article 34 of the Portuguese Constitution.

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

   According to article 18 of the Portuguese Constitution, the law may only restrict rights, freedoms and guarantees in cases expressly provided for in this Constitution, and such restrictions shall be limited to those needed to safeguard other rights and interests protected by this Constitution.

   Therefore, a limitation is only justifiable in terms of constitutional law if it is necessary to safeguard other rights or interests also protected by the Constitution.

   This necessity is evaluated in terms of the principle of proportionality.

   According to the Constitutional Court the principle of proportionality can be unfolded in three more specific principles:

   (i) the principle of adequacy, according to which limitations to rights, liberties and guarantees must be recognised as a mean to the pursuit of the ends envisaged, with the safeguard of other constitutional rights or goods involved;

   (ii) the principle of exigency, which requires that restrictive measures must be demanded in order to obtain the ends envisaged, as there are no other restrictive means available for achieving the same end;

   (iii) the principle of just measure, or proportionality in the strict sense, according to which no excessive measures can be adopted in order to obtain the ends envisaged.

   Article 9 of Law 32/2008 tried to reinforce this principle regarding the use of the data retained under the Directive.

According to this article, the judicial decision to provide data (to the competent authorities) must meet the requirements of adequacy, necessity and proportionality, namely as regards the categories of data provided and the competent authorities with access to data and the protection of professional secrecy, under the law.

10. Is the constitutionally fixed limit to a conferral of national sovereignties to the EU in any way binding for representatives of your country in EU organs and institutions (e.g. the Council of Ministers, the European Council) when exercising their functions in the adoption and execution of an EU legislative act?

Articles 3, 8 (4) and 277 (1) of the Portuguese Constitution, as well as the legal doctrine on the relationship between said Constitution and the secondary community legislation, need to be taken into consideration.

Pursuant to article 3 of the Constitution, the validity of laws is dependent on their conformity with the Constitution.

Therefore, rules that contravene any of the provisions of the Constitution or the principles included therein should be considered as unconstitutional under article 277 (1).

But according to article 8 of the Constitution, the rules issued by its institutions in the exercise of their respective responsibilities are applicable in the Portuguese internal law in accordance with Union law and with respect for the fundamental principles of a democratic state based on the rule of law.

Some of the Portuguese legal doctrine argues that the Portuguese Constitution should prevail over the secondary community legislation.

However, there are also those who believe that the secondary community legislation has supraconstitutional value.

In order for union law to be applicable in the internal legal system, and further supplant the Constitution, it is not necessary a constitutional provision saying so.

When Portugal entered into the European Community, the country accepted the latter's legal order and all of its existence requirements, the first being the primacy of the European law.

This doctrine invokes article 8 (3) of the Constitution to sustain this theory, where is stated that the rules issued by the competent bodies of international organisations to which Portugal belongs (EU) shall come directly into force in Portuguese internal law, on condition that this is laid down in the respective constituent treaties.

It is still a controversial issue widely discussed by the doctrine.

Prior review of constitutionality is, nonetheless, permitted by the Constitution under its article 278 but it is not a mandatory procedure.

The President of the Republic may ask the Constitutional Court to conduct a prior review of the constitutionality of any rule laid down by any decree that is sent to him for ratification as a law or executive law.

If the Constitutional Court pronounces the unconstitutionality of any rule contained in a decree, the President of the Republic must veto the concerned law and return it to the body that approved it.

Such decree may not be enacted or signed unless the body that passed it expunges the rule that has been deemed unconstitutional, or, where applicable, if said rule is confirmed by a majority that is at least equal to two thirds of all parliamentarians present and greater than an absolute majority of all the parliamentarians in full exercise of their office.

If the statute or treaty is reformulated, the President of the Republic may request the prior review of the constitutionality of any of the rules in the new version.

As referred, this is a right of the organs of sovereignty abovementioned but not an obligation.

11. **According to your answer to question 16 of the first questionnaire, Art. 9 para. 1 Law 32/2008 requires, for a data request to be justified, that the data is crucial for the to secure evidence in the scope of the investigation, detection, and prosecution of serious criminal offences (*crimes graves*). In your answer to question 15, you mention the categories of crimes covered by this term. Can you provide the legal source of this definition? Have these categories been narrowed down any further anywhere in the law (e.g. which crimes are considered a "terrorist crime")?**

No.

The interpreter will have to recur to the legal provisions applicable regarding each one of the types of crimes included in the definition of "serious crimes": *terrorist crime, violent crime, highly organized crime, illegal restraint, kidnapping and hostage taking, cultural identity or personal integrity crimes, crimes against national security, counterfeiting currency or equivalent securities, and crimes covered by conventions on safety of air and sea navigation*.

But they can found, although in order legal diplomas. This process may nonetheless raise doubts to the interpreter in our opinion.

a) Terrorism: Law 52/2003 dated of 22 August 2003 approved the Act to Combat Terrorism;

b) Violent crime: article 1, paragraphs j) and l) of the Code of Criminal Procedure contain the definitions of "violent crime" and "especially violent crime" as follows:

(i) "violent crime": criminal conducts that are intentionally target at people's life, physical integrity or freedom and are punishable by a maximum of 5 or more years of imprisonment;

(ii) "especially violent crime": criminal conducts that are intentionally target at people's life, physical integrity or freedom and are punishable by a maximum of 8 or more years of imprisonment;

c) Highly organized crime: : article 1, paragraph m) of the Code of Criminal Procedure defines "highly organized crime" as being a criminal conduct that involve one of the following crimes: criminal association, trafficking of people, trafficking of weapons, trafficking of narcotic drugs and psychotropic substances, corruption, improper influence and money laundering.

d) Illegal restraint: defined and sanctioned by article 158 of the Portuguese Penal Code.

e) Kidnapping and hostage-taking: defined and sanctioned by articles 161 and 162 of the Portuguese Penal Code.

f) Cultural identity or personal integrity crimes: Book II, Title III, Chapter II of the Portuguese Penal Code is entitled "cultural identity and personal integrity crimes", which defines and sanctions the following criminal offences: racial, religious or sexual discrimination (article 240), torture and other cruel, degrading or inhumane forms of existence (article 243) and aggravated torture and other cruel, degrading or inhumane forms of treatment (article 244).

g) Crimes against national security: Book II, Title V, Chapter I of the Portuguese Penal Code is entitled "crimes against national security", which defines and sanctions the following criminal offences: treason (article 308), espionage (article 317), disruption of means of evidence of national interest (article 318), diplomatic faithlessness (article 319), usurpation of Portuguese public authority (article 320), unlawful surrender of a person to a foreign entity (article 321), crimes against people that have international protection (article 322), insult to foreign symbols (article 323), violent alteration of rule of law (article 325), incitement to civil war and violent alteration of rule of law (article 326), attack against the President of the Republic (article 327), offence against the honour of the President of the Republic (article 328), sabotage (article 329), incitement to collective disobedience (article 330), links to foreign countries (article 331), insult to national and regional symbols (article 332), cohesive action against sovereign bodies (article 333), disruption to the functioning of a constitutional body (article 334), improper influence (article 335), falsification of voter registration (article 336), obstruction to obtain a valid voter card (article 337), disturbance of electoral assembly (article 338), electoral fraud (article 339), cohesive action against voter (article 340), voter's fraud and corruption (article 341), breach of the secret of the ballot (article 342).

h) Counterfeiting currency or equivalent securities: Book II, Title IV, Chapter II, Section III of the Portuguese Penal Code is entitled "counterfeiting money,

public credit and tax stamps", which defines and sanctions the following criminal offences: counterfeiting of money (article 262), alteration of the value of a coin (article 263), distribution of fake money agreed with the forger (article 264), distribution of fake money (article 265), acquisition of fake money to be put into circulation (article 266), securities similar to money (article 266) and counterfeiting of tax stamps (article 268).

12. **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. These rules do not exist.

13. **Please describe in detail the different steps that have to be taken by the involved bodies (judge, providers where the data is retained, requesting body, other authorities involved etc) upon a request for access to retained data. In particular: are there any technical specifications setting out how the SAPDOC software works in practice? If so, please describe their content. In particular: do they provide for measures in one or more of the following areas:**

- **access logging**
- **secure (irreversible) deletion after expiry**
- **error correction mechanisms (e.g. hash functions, checksums)**
- **secure data transmission (e.g. encryption algorithm used, safe custody of the crypto-keys)**
- **access/request procedure**
- **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)**

Information subject to data retention obligations, except for data on subscribers' names and addresses, is blocked as from the moment they are retained, and are only unblocked in order to be provided to the competent authorities.

All the information publicly available about how the SAPDOC system works is the following:

Through SAPDOC (an electronic application), the investigating judge completes a specific electronic form where he requests to providers the personal data covered by Law 32/2008.

Court judges access the software by introducing a user name and password.

The request for data includes: (1) the relevant court order that orders or authorizes transmission of data, in PDF or text file, bearing a digital signature and; (2) a electronic form completed in accordance with the court order aforementioned.

After entire completion of the aforementioned form by the judge, SAPDOC generates a PDF file where he further affixes his electronic signature.

With the electronic signature, the request is immediately sent to the providers.

Upon a receipt of a request for data, the provider shall immediately carry out the necessary search.

As soon as the data search is concluded, the provider transfers the file which corresponds to the search made through a secure and encrypted connection, authenticated with a user name and password, and also sends the notification of the reply file through the software, indicating the name of the transferred file.

The judge receives the encrypted file sent by the concerned providers, which may only be decoded by the digital signature card owned by the judge who sent the request in the first place.

The reply files abovementioned must be produced in PDF, must bear a digital signature and be encrypted by means of asymmetric keys made available through digital certificates. These files may only be viewed electronically through the software.

The provider is required to request, through the software, the rectification or completion of the request for data if the reasoned court order and data included by the judge in the electronic form do not match or if any of the elements of the request for data is missing.

The judge receiving the file (after decryption) should send it, whenever possible, by electronic means to the competent authorities that requested it.

The software notifies the service provider that the reply file was successfully received and stored.

Upon receiving this notification, the service provider may remove from his system the copy of the file sent to the judge. It is, however, required to continue to retain that data whenever required under Law 32/2008 (one year).

There must be electronic records of all data requests sent, with indication of who requested the access and the time and data they were sent as well as electronic record of all accesses to reply files, with the indication of who requested access and the respective time and date.

The judge orders, of his own motion or upon request by any interested party, the destruction of data held by competent authorities, as well as data preserved by providers, as soon as they are no longer required for their intended purpose. The data are deemed to be no longer required for their intended purpose in the following cases: (1) definitive closure of criminal proceedings; (2) final acquittal; (3) final conviction; (4) proceedings that becomes time-barred; and (5) amnesty.

The legal principles and rules on quality and safeguard of confidentiality and security data provided for in the Data Protection Law (which carried out transposition into national law of Directive 95/46/EC) and Law 41/2004 of 18 August (which carried out transposition of Directive 2002/58/EC) remain applicable in full.

However, we are unable to report on how these rules and principles are being implemented as no information is made available to the public.

14. In your answer to question 33 of the first questionnaire, you mention that there are no *specific* rules governing the co-operation between the bodies entitled to request access to retained data and other public bodies. Please explain how data exchange between these bodies is regulated in *general*, as far as these rules apply to retained data that have been accessed by an entitled body. Under which conditions may these data be transmitted to other bodies and for which purposes may they be used?

According to article 4-A (2) of Administrative Rule 694/2010, data made available by the judge to the competent agent may be used by judicial authorities or other competent authorities, specifically in the scope of the investigation, detection and prosecution of serious crimes, and may be converted or processed, in compliance with *leges artis*, under suitable conditions for their intended purposes.

This legal provision is rather unfortunate as it is extremely imprecise about under which conditions data transfer between the competent authorities may occur.

This subject-matter should not be included in an administrative rule as it is not of technical nature.

We can only assume that data exchange between these bodies, whenever admissible, will have to comply with the Portuguese Data Protection Law.

On the one hand, according to its article 8 (3), the processing of personal data for the purposes of police investigations shall be restricted to the process necessary to prevent a specific danger or to prosecute a particular offence or to exercise the responsibilities provided for in the respective implementing statutes or another legal

provision or in the terms of an international agreement or convention to which Portugal is a party.

On the other hand, central registers relating to persons suspected of criminal offences may only be created and kept by public services vested with that specific responsibility by virtue of the law establishing their organisation and functioning (so-called organic law), subject to observance of procedural and data protection rules provided for in a legal order, with the prior opinion of the Portuguese Data Protection Agency.

Therefore, data exchange between the so-called competent authorities may only take place if these requirements are met.

15. **Which EU legislative acts and international (multilateral) 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) apply to your country? Have bilateral agreements been concluded on data exchange with the U.S. (as far as they are relevant to data retained under Law 32/2008)?**

We are not aware of the existence of such agreements. Therefore, we may only provide information collected from the official authorities as follows:

• Europol Convention based in article K3 (2) (c) of the European Union Treaty (European Convention) which created the European Police Service. The Portuguese Data Protection Authority is legally in charge of monitoring compliance with the Convention's provisions.

• Law no. 109/2009, 15 of December, commonly known as Cybercrime law (hereinafter, "Cybercrime law") implemented the Convention on Cybercrime. The Portuguese authorities must cooperate with the competent foreign authorities for the purpose of criminal investigations or proceeding relating to computer systems or data, as well as the collection of evidence of a crime in electronic form, according to the rules on transfer of personal data contained in Law no. 67/98 (transposition of Directive 95/46/CE) (article 20 of Cybercrime law). For purposes of international cooperation, and in order to provide immediate assistance for the purposes aforementioned, *Polícia Judiciária* (Judiciary Police) is obliged to maintain a structure that guarantees a point of contact available at all times, twenty-four hours a day, seven days a week (article 21 of Cybercrime law).

• Resolution 63/2001 of the Portuguese Parliament dated October 2001 approved the 2000 European Convention on Mutual Assistance in Criminal Matters.

• Resolution 32/1999 of the Portuguese Parliament dated 21 April approved the Convention on the Use of Information Technology for Customs Purposes.

• Council of Europe Convention 108 for the Protection of Individuals with regard to Automatic Processing of Personal Data.

We are not aware of any other agreement that could be directly relevant for this question.

• But on 31 August 2011 the Parliament approved a proposal for a resolution ratifying the Agreement between Portugal and the USA, signed in Lisbon on 30 June 2009, to improve cooperation in the area of crime prevention and combat, in particular, as regards terrorism. In accordance with the Agreement, the two countries will be able to share certain information, pursuant to the respective national laws, in particular, they may provide fingerprints information, created for criminal prevention and investigation purposes, as well as DNA profiles.

16. As regards your answer to question 35 of the first questionnaire:

- **Does the Portuguese Data Protection Authority also have the competence to monitor compliance of the providers with the data retention obligations, as far as these obligations do *not* explicitly refer to the protection of personal data (e.g. the obligation to retain the data etc)? If not: which bodies are responsible for this task? Are these supervisory bodies independent in the sense of what has been said in question 35 of the first questionnaire?**

  The retention of data is considered to be a data processing activity. Therefore, all principles contained in the Portuguese Data Protection law are applicable.

  The only entity responsible for monitoring compliance of the providers is the Portuguese Data Protection Agency (CNPD) according to article 7, 8 and 14 of Law 32/2008. But this is an independent entity.

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

  No external bodies responsible besides the Portuguese Data Protection Agency (CNPD).