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

Malta

Prof. Kevin Aquilina

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, the provisions of the Directive have already been transposed into national law. This has been done by means of two Legal Notices, that is, two sets of regulations made under the provisions of two different laws.

The first subsidiary law which had to be amended to transpose the provisions of the Directive is called the *Processing of Personal Data (Electronic Communications*

Sector) Regulations, *2003*.[1] These regulations are part of the Laws of Malta and are numbered as Subsidiary Legislation (S.L.) 440.01. These regulations were made under Chapter 440 of the Laws of Malta, the *Data Protection Act*.[2] S.L. 440.01 was amended by Legal Notice 198 of 2008 entitled the *Processing of Personal Data (Electronic Communications Sector) (Amendment) Regulations, 2008*.[3] These 2008 regulations have transposed in part the Directive.

The second subsidiary law which had to be amended to transpose the provisions of the Directive is called the *Electronic Communications (Personal Data and Protection of Privacy) (Amendment) Regulations, 2003*.[4] These regulations are part of the Laws of Malta and are numbered as Subsidiary Legislation (S.L.) 399.25. These regulations were made under Chapter 399 of the Laws of Malta, the Electronic Communications (Regulation) Act.[5] S.L. 399.25 was amended by Legal Notice 199 of 2008 entitled the *Electronic Communications (Personal Data and Protection of Privacy) (Amendment) Regulations, 2008*.[6] These 2008 regulations have also transposed in part the Directive.

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

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

As the transposition has been accomplished, this question does not apply to the case of Malta.

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?

As the transposition has been accomplished, this question does not apply to the case of Malta.

---

1 See Document 1 attached.

2 See Document 2 attached.

3 See Document 3 attached.

4 See Document 4 attached.

5 See Document 5 attached.

6 See Document 6 attached.

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.**

   The two set of regulations quoted in the answer to paragraph 1 have not been amended since 2008. Nor has there been any court judgment which has annulled the 2008 regulations transposing the Directive into Maltese Law.

- ***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.**

   Yes, all the six documents referred to above are available on line at the www.justiceservices.gov.mt website as follows:

   - *Subsidiary Legislation 440.01 of the Laws of Malta –*

     http://www.justiceservices.gov.mt/LOM.aspx?pageid=27&mode=chrono&p=14&lawid=8906

   - *Chapter 440 of the Laws of Malta –*

     http://www.justiceservices.gov.mt/LOM.aspx?pageid=27&mode=chrono&p=14

   - *Subsidiary Legislation 399.25 of the Laws of Malta –*

     http://www.justiceservices.gov.mt/LOM.aspx?pageid=27&mode=chrono&p=13&lawid=8866

   - *Chapter 399 of the Laws of Malta –*

     http://www.justiceservices.gov.mt/LOM.aspx?pageid=27&mode=chrono&p=13

   - *Legal Notices 198 and 199 of 2008 –*

     http://www.justiceservices.gov.mt/LegalPublications.aspx?pageid=32&year=2008&type=4&p=8

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

   Both sets of regulations have been in force since 29 August 2008. No transition periods have been established in both regulations.

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.**

   Both legal notices 198 of 2008 and 199 of 2008 are subsidiary laws. In the Maltese legal system a primary act is an Act of Parliament. Such is the case of Chapters 399 and 440 of the Laws of Malta. In terms of these two enactments, it is possible for the competent Minister to make subsidiary legislation under the act of parliament by means of regulations. Regulations are binding at law. This is the main method of making subsidiary legislation. It corresponds to the method usually chosen in Malta for such kind of matters. The Data Protection Act is a law enacted by Parliament. In the case of the Data Retention Directive, the Government decided that it had ample powers under article 54 of the Data Protection Act to proceed by way of delegated legislation rather than through an amendment to the Data Protection Act. This is because it is faster to adopt a subsidiary law rather than an Act of Parliament. The latter takes more time to adopt.

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

   All the terms of article 2, paragraph 2 of the Directive have been transposed in regulation 17 of SL 440.01. The definitions have been transposed word for word, with no changes being made to them.

The other terms mentioned in the directives referred to by the Directive (see the reference made in art. 2 para. 1 of the Directive to Directives 95/46/EC, 2002/21/EC and 2002/58/EC) have also been legally defined in national legislation as follows:

in article 2 of the Data Protection Act with regard to Directive 95/46/EC;

in article 2 of the Electronic Communications (Regulation) Act and regulation 2 of the Electronic Communications Networks and Services (General) Regulations, S.L. 399.28 with regard to Directive 2002/21/EC;

in regulation 2 of the Electronic Communications Networks and Services (General) Regulations, S.L. 399.28 and the Electronic Communications (Personal Data and Protection of Privacy) Regulations, S.L. 399.25 with regard to Directive 2002/58/EC.

The other terms defined in regulation 17 of S.L. 440.01 are required from a domestic law perspective. These are: 'Police', 'security service' and 'serious crime'.

Dimension 1 (State - citizen)

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

The data which has to be retained according to the national rules transposing the directive are those set out in Article 5 of the Directive. Article 5 of the Directive has been faithfully transposed in regulations 20(1) and 18(3) of SL 440.01. The only difference in the transposition of Article 5 of the Directive is that the words 'Members States' have been correctly substituted by the words 'service providers'. Service providers are, in terms of regulation 18(1) of SL 440.01, 'a service provider of publicly available electronic communications services or of a public communications network'.

According to regulation 18 of SL 440.01, the data which has to be retained is that listed in regulation 20 above-mentioned irrespective of the provisions of regulations 4, 5, 6 and 7 of S.L. 440.01.

Regulation 4 prohibits the listening, tapping, storing or undertaking any other form of interception or surveillance of communications and of any related traffic data except in the case of public security agencies listed in regulation 10 which are authorised to carry out the above functions of listening, tapping, storing, etc. Regulation 4 is transposing Article 5 of Directive 2002/58/EC.

Regulation 5 regulates the access to information stored in terminal equipment. It transposes Article 5 of Directive 2002/58/EC.

Regulation 6 regulates traffic data. It transposes Article 6 of Directive 2002/58/EC.

Regulation 7 regulates location data. It transposes Article 9 of Directive 2002/58/EC.

The regulations do not include additional retention obligations with regard to traffic data that go beyond the obligations mentioned in the directive. This is because regulations 4, 5, 6 and 7 of S.L. 440.01 abovementioned are made subject to regulation 20 as regulation 18 starts off by using the words: "Notwithstanding the provisions of regulations 4, 5, 6 and 7". Therefore, these words mean that irrespective of whatever is written in regulations 4 to 7, it is regulation 20 which will prevail over these provisions.[7]

With regard to data on unsuccessful call attempts, the matter is dealt with by regulation 18(2) of S.L. 440.01 (transposing Article 3(2) of the Directive) which reads as follows:

"The obligation to retain the data as provided in sub-regulation (1) [that is the data specified in regulation 20 of S.L. 440.01 which transposes Article 5 of the Directive] shall, to the extent that such data are generated or processed, and stored (as regards telephony data) or logged (as regards internet data) be applicable to unsuccessful call attempts: Provided that such obligation shall not be applicable in relation to unconnected calls."

Hence there is an obligation to retain data relating to unsuccessful call attempts but not data relating to unconnected calls.

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.

Apart from the Security Services Act[8] and the Data Protection (Processing of Personal Data in the Police Sector Regulations),[9] national law provides for and allows for the retention of electronic communications data beyond that listed in Article 5 of the Directive as transposed in regulation 440.01. Such national law is contained in regulations 4, 5, 6 and 7 abovementioned which are made subject to

---

7 Please note that chronologically it is Legal Notice 198 of 2008 which was made first. It is a legal notice amending another Legal Notice. In fact L.N. 198 of 2008 has amended L.N. 16 of 2003. As the Laws of Malta are all numbered by the Law Commission (e.g. SL 440.01, SL 440.02, etc) when the Law Commission transforms a Legal Notice into a Subsidiary Law, it removes the first regulation of each regulation, that is regulation 1. Hence whilst in L.N. 198 of 2008 you have a first regulation setting out the title of the amending regulation, this is not needed when the amending regulation is consolidated into the principal regulation. The official version will be the principal regulation (SL 440.01) as amended by the amending regulation (LN 198 of 2008)

8 See Document 7.

9 See Document 8.

regulation 20 as regulation 18 starts off by using the words: "Notwithstanding the provisions of regulations 4, 5, 6 and 7". Therefore, these words mean that irrespective of whatever is written in regulations 4 to 7, it is regulation 20 which will prevail over these provisions.

Moreover, regulation 10 provides that regulations 4 to 7 do not apply to the public security agencies once these are specifically regulated by another law providing for the provision of information as a necessary measure in the interest of public security such as the Security Services Act and the Data Protection (Processing of Personal Data in the Police Sector) Regulations.[10]

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

According to regulation 19 of SL 440.01 (transposing Article 4 of the Directive), data is retained so that it can be disclosed only to the Police or to the Security Service, as the case may be, where such data is required for the purpose of the investigation, detection or prosecution of serious crime. According to regulation 17 of SL 440.01,

"Police" means the Commissioner of Police and includes any officer of the Police designated by the Commissioner to act of his behalf;

"security service" means the Security Service as defined in the Security Service Act;

"serious crime" means any crime which is punishable by a term of imprisonment of not less than one year and for the purposes of these regulations includes the crimes mentioned in articles 35(1)(d) and 35A of the Electronic Communications (Regulation) Act.

[10] A distinction has to be made between personal data which a service provider of publicly available electronic communications services or of a public communications network may retain and personal data – such as that collected under regulation 5(1) of SL 440.05 for historical purposes (regulation 7 of SL 440.05) by the Police Force without the assistance of a service provider of publicly available electronic communications services or of a public communications network, which data is (collected by and) retained by the Police. The same point applies to the Security Services when it is the Service itself which is collecting the data and retaining it (rather than a service provider of publicly available electronic communications services or of a public communications network collecting and retaining the data in question and subsequently passing it on to the Security Service).

12. Are there any specific rules in national law prohibiting the retention and/or transmission of sensitive data (i.e. data that is legally considered to be particularly worthy of protection, e.g. data resulting from a communication between individuals that are in a relationship of mutual trust particularly protected by law for reasons of overriding importance, as might be the case between a lawyer and his/her client, between a doctor and his/her patient, between a journalist and a whistle-blower)?[11]

Yes there are article 257 of the Criminal Code, Chapter 9 of the Laws of Malta, the Professional Secrecy Act,[12] Chapter 377 of the Laws of Malta and the Data Protection Act (see Document 2) prohibiting the retention and transmission of sensitive data.[13]

Article 257 of the Criminal Code reads as follows:

"**257.** If any person, who by reason of his calling, profession or office, becomes the depositary of any secret confided in him, shall, except when compelled by law to give information to a public authority, disclose such secret, he shall on conviction be liable to a fine (*multa*) not exceeding forty-six thousand and five hundred and eighty-seven euro and forty-seven cents (46,587.47) or to imprisonment for a term not exceeding two years or to both such fine and imprisonment:

Provided that, notwithstanding the provisions of any other law, it shall be a defence to show that the disclosure was made to a competent public authority in Malta or outside Malta investigating any act or omission committed in Malta and which constitutes, or if committed outside Malta would in corresponding circumstances constitute -

(*a*) any of the offences referred to in article 22(2)(*a*)(1) of the Dangerous Drugs Ordinance; or

---

11 In the case of traffic and location data of communications containing sensitive data, such traffic and location data would fall under the definition of 'sensitive personal data' and hence would be protected as such. Sensitive personal data is defined in article 2 of the Data Protection Act as '' and personal data is defined by the said article 2 as 'any information relating to an identified or identifiable natural person; an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social Identity.' The only case which allows blanket data retention in the sense that there is no need for a concrete crime to have been committed at the time of retaining the data is the Security Service Act which allows the Service (following authorization by the Minister responsible for the Security Service) to enter or interfere with property in certain cases listed in article 6 of the said enactment. However, according to article 10(1) a number of safeguards are established to ensure that the information obtained in terms of a warrant is kept confidential and article 10(2) further provides for the destruction of the information once its retention is no longer necessary.

12 See Document 9.

13 Sensitive personal data is defined by article 2 of the Data Protection Act as follows: ' "sensitive personal data" means personal data that reveals race or ethnic origin, political opinions, religious or philosophical beliefs, membership of a trade union, health, or sex life.'

(*b*) any of the offences referred to in article 120A(2)(a)(1) of the Medical and Kindred Professions Ordinance; or

(*c*) any offence of money laundering within the meaning of the Prevention of Money Laundering Act:

Provided further that the provisions of the first proviso of this article[14] shall not apply to a person who is a member of the legal or the medical profession."

The Professional Secrecy Act is attached as Document 9.

Article 12 of the Data Protection Act regulates sensitive personal data and prohibits the processing of sensitive data except in certain cases. It reads as follows:

"**12.** (1) Subject to the other provisions of this Act no person shall process sensitive personal data:

Provided that such personal data may be processed in those cases provided for under subarticle (2) and under articles 13 to 16 or as may be prescribed by the Minister having regard to an important public interest.

(2) Sensitive personal data may be processed if the data subject:

(*a*) has given his explicit consent to processing; or

(*b*) has made the data public."

The word 'processing' is defined in article 2 of the Data Protection Act and means:

"any operation or set of operations which is taken in regard to personal data, whether or not it occurs by automatic means, and includes the collection, recording, organisation, storage, adaptation, alteration, retrieval, gathering, use, disclosure by transmission, dissemination or otherwise making information available, alignment or combination, blocking, erasure or destruction of such data".

Article 13 of the Data Protection Act regulates necessary processing of sensitive personal data. Article 13 reads as follows:

---

[14] The first proviso to article 257 of the Criminal Code reads as follows:

Provided that, notwithstanding the provisions of any other law, it shall be a defence to show that the disclosure was made to a competent public authority in Malta or outside Malta investigating any act or omission committed in Malta and which constitutes, or if committed outside Malta would in corresponding circumstances constitute -

(*a*) any of the offences referred to in article 22(2)(*a*)(1) of the Dangerous Drugs Ordinance; or

(*b*) any of the offences referred to in article 120A(2)(a)(1) of the Medical and Kindred Professions Ordinance; or

(*c*) any offence of money laundering within the meaning of the Prevention of Money Laundering Act:

"**13.** Sensitive personal data may be processed if appropriate safeguards are adopted and the processing is necessary in order that:

(*a*) the controller will be able to comply with his duties or exercise his rights under any law regulating the conditions of employment; or

(*b*) the vital interests of the data subject or of some other person will be able to be protected and the data subject is physically or legally incapable of giving his consent; or

(*c*) legal claims will be able to be established, exercised or defended.".

Should these two articles be infringed, then there is a criminal sanction established in article 47(1)(b) of the Data Protection Act. Article 47(1) of the Data Protection Act reads as follows:

"**47.** (1) Any person who:

(*a*) provides untrue information to data subjects as is prescribed by this Act, or in the notification to the Commissioner under article 29 or to the Commissioner

when the Commissioner requests information in accordance with article 41;

(*b*) processes personal data in contravention of the provisions of articles 12 to 17;

(*c*) transfers personal data to a third country in contravention of article 27 and 28;

(*d*) omits to give notification under article 29(1) or in accordance with regulations issued under article 34;

shall be guilty of an offence and shall on conviction be liable to a fine (*multa*) not exceeding twenty-three thousand and two hundred and ninety-three euro and seventy-three cents (€23,293.73) or to imprisonment for six months or to both such fine and imprisonment."

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

Regulation 21 of SL 440.01 establishes the retention periods. It transposes Article 6 of the Directive. The categories of data specified in regulation 20 have to be retained by the service providers for the following periods:

communication data relating to Internet Access and Internet e-mail for a period of six months from the date of communications;

communications data concerning fixed network telephony, mobile telephony and Internet telephony for a period of one year from the date of communication.[15]

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

According to regulation 19 of SL 440.01 transposing Articles 4 and 11 of the Directive, it is only the Police and the Security Service who have access to data.

15. For which purposes may the data retained be used according to the national law transposing the Directive, for which purposes may they be used according to other national law (e.g. for law enforcement (criminal/administrative offences), security, civil action (e.g. to enforce copyright claims))? Does the national law grant any rights to individuals to access the data retained directly, e.g. in a civil action (right to information on the owner of an IP address)?

The purposes for which the data retained may be used according to national law are set out in regulation 19(1) of SL 440.01. These are "for the purpose of the investigation, detection or prosecution of serious crime". Regulation 19 does not grant the right to individuals to access the data retained in terms of the Processing of Personal Data (Electronic Communications Sector) Regulations, SL 440.01.

Moreover, in terms of regulation 5(1) of S.L. 440.05, "the collection of personal data for police purposes shall be such as is necessary for the prevention, suppression, investigation, detection and prosecution of specific criminal offences or for the prevention of real danger, or as specified in any law." Furthermore, regulation 5(4) of S.L. 440.05 stipulates that the "processing of sensitive personal data is allowed if this is necessary for the purposes of a particular inquiry."

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

Regulation 19(1) of S.L. 440.01 requires a "serious crime". Although not mentioned in regulation 19(1), it is obvious that the "serious crime" is still a suspected serious crime because the words "serious crime" are qualified in regulation 19(1) by the words "investigation, detection or prosecution". In all these three stages, the serious crime is still suspected as the stage of a criminal trial has not yet been reached, if it will ever be reached for there is also the possibility that no criminal charge is instituted before a court of criminal justice.

---

[15] Although the law does not explain the difference in the period of retention between the two categories, usually the Police and Security Service find it more effective to resort to communication data concerning telephony and hence the period of retention for such category is longer than that for e-mail. Indeed, there have been cases prosecuted in court where the Police have relied on telephone intercepts carried out by the Security Service and such intercepts have been brought as evidence in court. I am not however aware of cases where the evidence was in the form of intercepterd e-mails.

See also regulation 5(1) and (4) cited in the previous reply.

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?

No, there are no such requirements under S.L. 440.01 However, reference has to be made to regulation 5(2) of S.L. 440.05 which provides that: "Without prejudice to article 23[16] of the [Data Protection] Act,[17] where personal data has been processed without the knowledge of the person concerned, the data subject should only be informed where practicable, that information is held about him, as soon as the object of the police activities is no longer likely to be prejudiced, and if the data are not deleted."

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?

No, there is no requirement of a priori or a posteriori notification to the aggrieved party under S.L. 440.01. But see regulation 5(2) of S.L. 440.05 quoted in the reply to question 17.

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

No, SL 440.01 does not establish any such requirement. However, regulation 5(2) of the Data Protection (Processing of Personal Data in the Police Sector) Regulations, S.L. 440.05, provides for post-facto information to the aggrieved party. It reads as follows:

"Without prejudice to article 23 of the Act, where personal data has been processed without the knowledge of the person concerned, the data subject should only be informed, where practicable, that information is held about him, as soon as the object of police activities is no longer likely to be prejudiced, and if the data are not deleted."

Article 23 of the Data Protection Act provides that:

---

16 See answer to question 19 for the text of article 23 of the Data Protection Act.

17 Regulation 5 of SL 440.05 states that where personal data has been processed without the knowledge of the person concerned, the data subject has to be informed that information is held about him as soon as the object of the police activities are no longer likely to be prejudiced and if the data is not deleted. However, regulation 5 of SL 440.05 does not apply to the cases listed in article 23 of the Data Protection Act (national security, defence, public security, etc.). In these cases, the data subject is not entitled to be informed that his personal data has been processed and that police investigations had been carried in his respect, even if such investigations have been concluded. Article 23 of the Data Protection Act is transposing Article 3(2) of Directive 95/46/EC.

"**23.** (1) The provisions of articles 7, 19, 20 (1), 21 and 35 shall not apply when a law specifically provides for the provision of information as a necessary measure in the interest of:

(*a*) national security;

(*b*) defence;

(*c*) public security;

(*d*) the prevention, investigation, detection and prosecution of criminal offences, or of breaches of ethics for regulated professions;

(*e*) an important economic or financial interest including monetary, budgetary and taxation matters;

(*f*) a monitoring, inspection or regulatory function connected, even occasionally, with the exercise of official authority referred to in paragraphs (*c*), (*d*) and (*e*); or

(*g*) such information being prejudicial to the protection of the data subject or of the rights and freedoms of others.

(2) The provisions of article 21 shall not apply when data is processed solely for purposes of scientific research or is kept in personal form for a period which does not exceed the period necessary for the sole purpose of compiling statistics:

Provided that the provisions of this subarticle shall not apply where the data is used for taking measures or decisions regarding any particular individual or where there is a risk of breaching the privacy of the data subject.".

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

S.L. 440.01 does not provide any right for an aggrieved party to have recourse to the courts.

Compensation for damages suffered by the data subject against the controller are regulated by Article 46 of the Data Protection Act which provides as follows:

'46. (1) The data subject may, by sworn application filed in the competent court, exercise an action for damages against the controller who processes data in contravention of this Act or regulations made thereunder.

(2) An action under this article shall be commenced within a period of twelve months from the date when the data subject becomes aware or could have become aware of such a contravention, which ever is the earlier.'

The data subject has a right of access, rectification and appeal in terms of regulation 13 of the Data Protection (Processing of Personal Data in the Police Sector) Regulations, S.L. 440.05. But this right is limited only to rectification of data on the aggrieved party rather than on unlawful data access or processing operations. This provision reads as follows:

"**13.** (1) The data subject may request in writing the following from the controller:

(*a*) whether personal data is being processed about him for a stated purpose,

(*b*) rectification, blocking or erasure of data that has not been processed in accordance with these regulations.

(2) Without prejudice to article 23 of the Act, the controller shall provide the data subject with information in accordance with article 21(2) of the Act and rectify, block or erase personal data subject to article 22 of the Act and without excessive delay and without expense. Provided that:

(*a*) the rights of access, rectification and blocking are not restricted or refused in accordance with subregulation 3, or

(*b*) in the interest of the data subject, there is no other law excluding the provision of information.

(3) The exercise of the rights of access, rectification and blocking or erasure by the data subject, shall only be restricted or refused insofar as the restriction or refusal is justified for the purpose of the suppression of criminal offences, or is necessary for the protection of the data subject or the rights and freedom of others.

(4) The data subject shall be informed in writing of the decision imposing a restriction or refusal to the exercise of the rights mentioned in subregulation (3) and shall include reasons for the restriction or refusal:

Provided that it shall be lawful not to communicate the said reasons if such restriction or refusal to communicate reasons is necessary for the performance of a legal task of the police or is necessary for the protection of the rights and freedom of others.

(5) Where access, rectification or erasure are refused or restricted, the data subject shall be entitled to appeal to the Commissioner for Data Protection within thirty days from when the data subject is informed, or may reasonably be deemed to have known, of the decision.

(6) In considering the appeal the Commissioner for Data Protection shall review the decision and shall satisfy himself that the refusal or restriction is reasonable and well founded."

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

Article 47 of the Data Protection Act prohibits unauthorised access to the data retained whilst processing and the definition of the term "processing" is wide enough to include access to the data retained.

Regulation 14 of S.L. 440.05 provides also that:

"14. (1) The controller [Commissioner of Police or his representative, or any other head of a public authority or body exercising police powers or his representative such as the Security Service, as the case may be] shall implement appropriate technical and organisational measures to protect the personal data that are processed against accidental destruction or loss or unlawful forms of processing thereby providing an adequate level of security that gives regard to the:

technical possibilities available;

cost of implementing the security measures;

special risks that exist in the processing of personal data;

sensitivity of the personal data being processed.

(2) Where the controller engages a processor, the controller shall ensure that the processor:

(a) can implement the security measures that must betaken;

(b) actually takes the measures so identified by the controller."

This regulation applies only to the Police and to the Security Service and not to service providers. In so far as service providers are concerned, the matter is regulated by regulation 23 of SL 440.01 which reads as follows:

'23. Data retained under this Part shall comply with the data security principles established under the Act (see in particular article 7 of the Data Protection Act) and shall as a minimum –

be of the same quality and subject to the same security and protection as the data on the network;

be subject to appropriate technical and organisational measures to protect the data against accidental or unlawful destruction, accidental loss or alteration, or unlawful storage, processing, access or disclosure;

be subject to appropriate technical and organisational measures to ensure that they can be accessed by specially authorised personnel only;

except for such data as are the subject of a conservation order be destroyed at the end of the applicable retention period.

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

S.L. 440.01 does not establish any time period within which the Police and/or the Security Service have to destroy the data transmitted to them by the service provider. This is because regulation 21 (which transposes Article 6 of the Directive) and deals with the period of retention applies to service providers and not to the Police and the Security Service. Hence no time limit for the destruction of the data is established by S.L. 440.01.

However, regulation 6(3) of the Data Protection (Processing of Personal Data in the Police Sector) Regulations, S.L. 440.05 provides that "Personal data processed for police purposes shall not be kept for a period longer than is necessary having regard to the police purposes for which they are processed."

Dimension 2 (State – economy)

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

According to article 3 of SL 440.01, these regulations apply to "the provision of publicly available electronic communications services in public communications networks in Malta".

In Document 5, the word "service provider" is also used although the law does not define the term. However, from the context of the regulations, it can be declared that the service provider has to be an undertaking which provides publicly available electronic communications services.

The words "public communications network," "electronic communications network" and "electronic communications service" are also defined in Document 5 as follows:

"public communications network" means an electronic communications network used wholly or mainly for the provision of publicly available electronic communications services;

"electronic communications network" means transmission systems and, where applicable, switching or routing equipment and other resources which permit the conveyance of signals by wire, by radio, by optical or by other electromagnetic means, including satellite networks, fixed (circuit-switched and packet-switched, including Internet) and mobile terrestrial networks, electricity cable systems, to the

extent that they are used for the purpose of transmitting signals, networks used for radio and television broadcasting, and cable television networks, irrespective of the type of information conveyed;

"electronic communications service" means a service normally provided for remuneration which consists wholly or mainly in the conveyance of signals on electronic communications networks, including telecommunications services and transmission services in networks used for broadcasting, but exclude services providing, or exercising editorial control over, content transmitted using electronic communications networks and services; it does not include information society services, as defined in the Electronic Commerce Act, which do not consist wholly or mainly in the conveyance of signals on electronic communications networks;

According to regulation 19(2) of SL 440.01, the data has to be retained and access is to be given to the Police and Security Service by "a service provider [that is, an undertaker] of publicly available electronic communications services or of a public communications network".

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 there is no such exemption contemplated in regulation 19 of S.L. 440.01. All service providers are placed in the same category.

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

There is no published information of which I am aware of that sheds light on the situation prior to 29 August 2008 as the law did not regulate this matter. It was therefore within the discretion of each service provider to adopt its own policies in this regard once the matter was unregulated.

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

Yes, the matter is dealt with by regulation 14 of the Data Protection (Processing of Personal Data in the Police Sector) Regulations, S.L. 440.05. See answer to question 21 for the text of regulation 14 of S.L. 440.05 and of regulation 23 of SL 440.01 which applies to service providers.

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)?

I have not come across any published information which answers this question.

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?

S.L. 440.01 does not empower the Government to reimburse costs for the implementation of the Directive. All such costs have to be borne by the service providers themselves.

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

Regulation 19 of S.L. 440.01 does not provide any rules for co-operation between the service providers and the Police/Security Services. It simply states that the service providers have to provide the data "without undue delay" following a request to that effect which has to be made in writing, has to be clear and specific. However, where the data is urgently required by the Police and/or the Security Service, the request can be made orally but a written request has to be follow "at the earliest opportunity".

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

If the service providers do not comply with the data retention provisions they will be in breach of article 47 of the Data Protection Act.[18] A civil action for tortuous liability may also be instituted by the aggrieved party under the general provisions of civil law as contained in the Civil Code.

---

[18] Art 47 applies to a violation of data protection rules only. There is another provision foreseeing similar sanctions also in the case that the service provider fails to fulfil the obligations to retain traffic and location data and to transfer them to the competent authorities upon request. This provision is found in regulation 13 of SL 440.01 which reads as follows:

'13. Any person who contravenes or fails to comply with these regulations shall be liable to an administrative fine not exceeding twenty-three thousand and two hundred and ninety-three euro and seventy-three cents (23,293.73) for each violation and two thousand and three hundred and twenty-nine euro and thirty seven cents (2,329.37) for each day during which such violation persists, which fine shall be determined and imposed by the Commissioner.'

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?

In terms of regulation 19(1) of S.L. 440.01 there are two such public bodies: the Police and the Security Service. The Security Service is headed by an Assistant Commissioner of Police and has its Headquarters at the Police Headquarters.

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

No there are no such regional entities which are empowered to access data.

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

The two bodies which can access the data are the Police and the Security Service. The Security Service is run mainly by the Police. Since its establishment in 1995, the Head of the Security Service has been a Police Officer, either the Commissioner of Police or one of his Assistant Commissioners of Police. Prior to 1995, Security Service functions were carried out by the Police. Moreover, both the Police and the Security Service function from the same premises and both use members of the Police Force to carry out their duties. No general rules of co-operation need to be adopted because although the organisations are two, in reality they function more as one.

Regulation 8 of S.L. 440.05 provides that:

"(1) The communication of personal data between different bodies exercising police powers shall only be permitted where there exists a legitimate interest for such communication within the framework of the legal powers of such bodies.

(2) Communication of personal data from bodies exercising police powers, to other Government Departments or to bodies established by law, or to other private parties may only be made in accordance with regulation 10 if:

(a) there exists a legal obligation or authorisation to communicate such data; or

(b) the Commissioner for Data Protection authorises such communication of data.

(3) In exceptional cases, communication of personal data from bodies exercising police powers, to other Government Departments or to bodies established by law, or to other private parties, may also be made if:

(a) it is clearly in the interest of the data subject and either the data subject himself has consented to the communication or circumstances are such as to allow a clear presumption of such consent; or

(b) it is necessary for the prevention of a serious and imminent danger.

(4) Bodies exercising police powers may also communicate personal data to other Government Departments or bodies established by law,[19] if the data are necessary for the recipient to enable him to fulfil his lawful task and provided that the purpose of the processing to be performed by the recipient is not incompatible with the original processing or contrary to the legal obligations of the body exercising police powers."

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

In so far as exchange of retained data with other EU Member States, the matter is regulated by regulations 9 and 10 of the Data Protection (Processing of Personal Data In The Police Sector) Regulations, S.L. 440.05.

According to regulation 3 of S.L. 440.05, these regulations "apply to public bodies exercising police powers" and according to regulation 2 of the same regulations "for Police Purposes" means "all the tasks which the police (or other public entities, authorities or bodies exercising police powers) must perform for the prevention and suppression of criminal offences or the maintenance of public order." The Security Service also falls within this definition in terms of its functions as outlines in article 3(2) and (3) of the Security Service Act, Chapter 391 of the Laws of Malta.[20] Hence in so far as Malta is concerned, S.L. 440.05 applies both to the Police and to the Security Service.

In terms of regulation 9 of S.L. 440.05, "transfer of data to foreign authorities may only be made in accordance with regulation 10 and if the recipients of such data are bodies exercise police powers." Furthermore, "such transfer of data shall only be permissible if there exists a legal obligation under any law, or an international

---

[19] This means that the retained data, once they have been accessed by the Police or the Security Service, may be shared with other public bodies under the conditions laid down in this paragraph.

[20] See Document 9.

obligation under a treaty, convention or international agreement on mutual assistance, to which Malta is a party." However, in the absence of such a provision, "transfer of data to foreign authorities may also be made if such communication is necessary for the prevention of a serious and imminent danger, or is necessary for the suppression of a serious criminal offence."

Requests for communication of personal data by foreign authorities are regulated by regulation 10 of S.L. 440.05. It is to be noted that the words "foreign authorities" are not defined. Hence they have to be applied to any foreign authority, irrespective of whether such authority is an authority of an E.U. Member State, E.E.A. Member State or a third country.

Regulation 9 thus enables a foreign authority to access data held by the Police and Security Service on the basis of an agreement or, in exceptional circumstances, for the prevention of a serious and imminent danger or for the suppression of a serious crime.

The foreign authorities do not enjoy a right to avail themselves to access the retained data directly but must request such information "in writing to the body exercising police powers, and shall include an indication of the person or body making the request and of the reason and purpose for which the request is made unless any other law or any international agreement to which Malta is a party, provides otherwise."

The national authorities responsible for cross-border data exchange are the Police and the Security Service. Maltese Law is silent as to the procedure when the Police and Security Service request the transfer of personal data to them from a foreign authority. The procedure in regulation 9 of SL 440.05 does not apply to outgoing requests for data retained in another country. In such cases, the matter would have to be dealt with by the national law of the foreign authority which would be in possession of the said data. The Maltese authorities, in drawing up their request, will have to comply with the requirements of foreign national law.

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

The Data Protection Act is administered by the Information and Data Protection Commissioner. Such a Commissioner administers two laws– the Freedom of Information Act (which is still in the process of coming fully into force) and the Data Protection Act (which has been in force since 2002). According to regulation 12 of S.L. 440.01, the said Commissioner 'shall ensure compliance with the provisions of these regulations.' This is basically the transposition of Article 9 of the

Directive (supervisory authority) into Maltese Law. The regulations retain the same supervising authority for all data protection related matters, both under the Data Protection Act and in these regulations.

In terms of article 36 of the Data Protection Act, the Information and Data Protection Commissioner is appointed by the Prime Minister after he has consulted the Leader of the Opposition. In terms of article 37(1) of the Data Protection Act, the office of Commissioner is established as an independent office and in the exercise of his functions the Commissioner acts independently and is not subject to the direction or control of any other person, be it the Prime Minister or a Minister of Government or authority, be it Parliament or Cabinet. The Commissioner thus acts with complete independence both in law and in practice and does not exercise his functions under the supervision or control of a superior authority or ministry.

The only supervision applied over the Commission is one of a quasi-judicial and judicial nature. The quasi-judicial supervision comes in terms of article 48 of the Data Protection Act in the form of an Information and Data Protection Appeals Tribunal and judicial supervision comes in terms of article 51 of the Data Protection Act in the form of an appeal from the said Tribunal to the Court of Appeal.

The appeal to the Court of Appeal is limited to a point of law only (hence points of fact are excluded) but in the case of an appeal from the Commissioner's decision to the Tribunal the appeal can be lodged both on a point of fact and a point of law (article 49(2) of the Data Protection Act).

The Court of Appeal is composed of one Judge. The Tribunal Chairman has to be an advocate with a minimum of twelve years legal experience, that is, an advocate who, in terms of the Constitution of Malta, may be appointed Judge of the Superior Courts.

The Commissioner, in terms of article 39(2) of the Data Protection Act, enjoys security of tenure whilst in office and can be removed only in the same way as judges and magistrates may be removed from office, that is, following an address by the Prime Minister to the House of Representatives supported by the votes of not less than two thirds of all the members thereof and praying for such removal on the ground of proved inability to perform the functions of his office (whether arising from infirmity of body or mind or any other cause) or proved misbehaviour. The Tribunal can exercise supervisory control over the Commissioner both in terms of legality (points of law) and technical advisability (points of fact) but the Court of Appeal can exercise supervision only with regard to control of legality (points of law).

II. Relevant case-law

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

No such lawsuits or administrative proceedings have been instituted or commenced.

If so, please answer to the following questions:

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

Not applicable.

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

Not applicable.

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

Not applicable.

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

No such lawsuits have been commenced.

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

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

There is no published information which states where is the data stored. But industry practice is to store data in electronic format at the service provider's premises. They are stored at a centralised level.

39. Are data stored outside the country or would this be permissible according to national law? If either of these cases applies: what data protection rules have

the companies involved in the storage (both in your country and abroad) been obligated to?

Data is stored in Malta, not abroad. There is however no prohibition in the law disallowing data from being stored abroad even if this is not the current practice. There are no requirements as to the level of data protection that has to be ensured when storing data abroad. Nor does the law limit data storage in any third country or to other EU Member States. In fact, in terms of article 4, the territorial scope of the Act is limited only to Malta except in the cases of:

(a) … the processing of personal data carried out in the context of the activities of an establishment of a controller in Malta or in a Maltese Embassy or High Commission abroad;

(*b*) … the processing of personal data where the controller is established in a third country provided that the equipment used for the processing of the personal data is situated in Malta.

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

a) no data are retained beyond what is permitted?

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

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

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

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

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

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

Regulation 4A of the Electronic Communications (Personal Data and Protection of Privacy) Regulations, S.L. 399.25, provides that:

"It shall be the obligation of a service provider to ensure that it has in place the necessary technical and administrative capacity and all other requirements to enable it to comply with the provisions of regulations 19 [regarding access to data] and 21 [regarding periods of retention] of the Processing of Personal Data (Electronic Communications Sector) Regulations, [S.L. 440.01] for the purposes of grating access to data as established in regulation 20 [regarding the categories of data to be retained] of the said regulations and to retain such data for such periods as established by regulation 22(a) and (b) of the said regulations."

In other words, though service providers have an obligation to retain data for such time as prescribed by regulation 22, to retain such categories of data as prescribed by regulation 20, and to grant access to such data as prescribed by regulation 19 of S.L. 440.01, regulation 4A of S.L. 399.25 does not prescribe the form of the technical and administrative capacity which service providers have to comply with. The only guideline is that given in regulation 19 of S.L. 440.01 which requires such data to be provided in "an intelligible form and in such a way that it is visible and legible". Hence the data cannot be provided as raw data but as processed data and cannot be provided in encoded form but has to be provided in unencoded form.

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)?

Although regulation 4A does not define what technical and administrative capacity service providers should comply with, the Data Protection Commissioner, in terms of regulation 12 of S.L. 440.01, has to ensure compliance with these regulations. So it is his office which has to see what technical and administrative capacity is in place. However, provided that there is some form of technical and administrative capacity in place, the Commissioner cannot really do much more than ascertain that such capacity is in place. He does not have the right to approve such capacity before it is put in place or request changes to be made to such capacity once in place.

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?

There is no published information which sheds light on the information requested above. However, regulation 14 refers to security measures relating to processing. See answer to question 21 for the text of regulation 14 of S.L. 440.05.

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

There is no published information which sheds light on the information requested above. However, reference should be made to regulation 19 of SL 440.01. See answer to question 29 for the text of regulation 14 of S.L. 440.05.

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

In so far as third countries are concerned, that is a country which is not an E.U. Member State, requests for the transfer of personal data have to comply with the provisions of articles 27 and 28 of the Data Protection Act and the Third Country (Data Protection) Regulations, S.L. 440.03.[21] In terms of regulation 5 of S.L. 440.03, prior to transferring personal data to a third country, "data controllers shall notify the Commissioner of any transfer of data resulting from a processing operation." In so far as *outgoing* requests for data retained in other countries is concerned, the matter has to be handled in terms of the foreign country's national law.

Articles 27 and 28 of the Data Protection provide as follows:

"**27.** (1) Without prejudice to the provisions of article 28, the transfer to a third country of personal data that is undergoing processing or intended processing, may only take place subject to the provisions of this Act and provided that the third country to which the data is transferred ensures an adequate level of protection.

(2) The adequacy of the level of protection of a third country shall be assessed in the light of all the circumstances surrounding a data transfer operation or a set of data transfer operations; particular consideration shall be given to the nature of the data, the purpose and duration of the proposed processing operation or operations, the country of origin and country of final destination, the rules of law, both general and sectoral, in force in the third country in quest ion and the professional rules and security measures which are complied with in that country.

(3) It is for the Commissioner to decide whether a third country ensures an adequate level of protection.

(4) The transfer of personal data to a third country that does not ensure adequate protection is prohibited.

28. (1) For the purpose of implementing any international convention to which Malta is a party or any other international obligation of Malta, the Minister may by Order designate that the transfer of personal data to any country listed in the said

[21] See Document 10.

Order shall not, notwithstanding the provisions of this Act or any other law, be restricted on grounds of protection of privacy. In making such Order the Minister may include conditions and restrictions provided for in any said international instrument.

(2) A transfer of personal data to a third country that does not ensure an adequate level of protection within the meaning of article 27(2) may be effected by the controller if the data subject has given his unambiguous consent to the proposed transfer or if the transfer -

(*a*) is necessary for the performance of a contract between the data subject and the controller or the implementation of precontractual measures taken in response to the data subject's request;

(*b*) is necessary for the performance or conclusion of a contract concluded or to be concluded in the interests of the data subject between the controller and a third party;

(*c*) is necessary or legally required on public interest grounds, or for the establishment, exercise or defence of legal claims;

(*d*) is necessary in order to protect the vital interests of the data subject; or

(*e*) is made from a register that according to laws or regulations is intended to provide information to the public and which is open to consultation either by the public in general or by any person who can demonstrate legitimate interest, provided that the conditions laid down in law for consultation are fulfilled in the particular case.

(3) Without prejudice to subarticle (1) the Commissioner may authorise a transfer or a set of transfers of personal data to a third country that does not ensure an adequate level of protection within the meaning of article 27(2):

Provided that the controller provides adequate safeguards, which may result particularly by means of appropriate contractual provisions, with respect to the protection of the privacy and fundamental rights and freedoms of individuals and with respect to their exercise."

B. National (societal) context

45. In general, is society aware of the public surveillance measures adopted in your country? How are these measures assessed by citizens, economy, the government and other public bodies? Please describe the public debate on the introduction (and, if corresponding rules have existed before the Directive entered into force, also on the amendment) of data retention in your country. Please illustrate the situation as comprehensively as possible, i.e. differentiating by political and social groups (political parties, civil rights groups, labour

unions as well as other professional organisations of the professions concerned (police officers, judges, lawyers/attorneys), consumer and business associations, the media, etc), and by the parties involved (businesses, data protection officers, law enforcement agencies, government representatives).

There has been no public debate on the transposition of the Directive into Maltese Law. It is therefore difficult to say how these measures are assessed by citizens, the economy, government and other public bodies. Nor has there been or is there any public debate on the public surveillance measures adopted in Malta. Public surveillance has not been an issue in Malta.

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

There are no obligations to retain personal data without a *specific* reason. For data to be retained it must be "necessary for the prevention, suppression, investigation, detection and prosecution of specific criminal offences or for the prevention of real danger, or as specified in any law." (regulation 5(1) of S.L. 440.05).

Regulation 5(1) of S.L. 440.05 refers to the Police and the Security Service only. Data retention obligations, however, may also be imposed on private actors, as is the case with electronic communications data retention, where service providers are obliged to store the data. Other data retention obligations existing in Malta, whether the obligated party be a public or a private body, are found in regulations 18 to 23 of SL 440.01. Moreover, regulation 4A of the Electronic Communications (Personal Data and Protection of Privacy) Regulations – SL 399.25 – states that:

'4A. It shall be the obligation of a service provider to ensure that it has in place the necessary technical and administrative capacity and all other requirements to enable it to comply with the provisions of regulations 19 and 21 of the Processing of Personal Data (Electronic Communications Sector) Regulations, for the purposes of granting access to data as established in regulation 20 of the said regulations and to retain such data for such periods as established by regulation 22(*a*) and (*b*) of the said regulations.'

The only case which allows blanket data retention in the sense that there is no need for a concrete crime to have been committed at the time of retaining the data is the Security Service Act which allows the Service (following authorization by the Minister responsible for the Security Service) to enter or interfere with property in certain cases listed in article 6 of the said enactment. However, according to article 10(1) a number of safeguards are established to ensure that the information obtained in terms of a warrant is kept confidential and article 10(2) further provides for the destruction of the information once its retention is no longer necessary.

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.

I am not aware of the publication of any such statistics.

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?

I am not aware of the publication of any 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 information that such discussions have or are taking place.

C. National constitutional/legal framework

I. Dimension 1 (State – citizen)

50. Which national fundamental rights protecting privacy, personal data and the secrecy of telecommunications do exist in your country? Are there any other fundamental rights granted to citizens that could be affected by data retention (e.g. freedom of expression and information/freedom of the media, freedom of thought, religion/belief and/or conscience, judiciary basic rights, freedom of profession in cases where the confidentiality of communication is essential etc)? Do the fundamental rights mentioned result from the constitution, from other legal acts or from case-law? Please describe the scope of protection of these fundamental rights. As regards the right to secrecy of telecommunications: Which data are – according to national (constitutional) law[22] – considered as telecommunications content? Is it legal under national (constitutional) law to retain this content without a specific reason?

The Constitution of Malta (see Document 11) contains a provision regulating the protection for privacy of home or other property in article 38 thereof. It reads as follows:

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

"**38.** (1) Except with his own consent or by way of parental discipline, no person shall be subjected to the search of his person or his property or the entry by others on his premises.

(2) Nothing contained in or done under the authority of any law shall be held to be inconsistent with or in contravention of this article to the extent that the law in question makes provision -

(*a*) that is reasonably required in the interest of defence, public safety, public order, public morality or decency, public health, town and country planning, the development and utilisation of mineral resources, or the development and utilisation of any property in such a manner as to promote the public benefit;

(*b*) that is reasonably required for the purpose of promoting the rights or freedoms of other persons;

(*c*) that authorises a department of the Government of Malta, or a local government authority, or a body corporate established by law for a public purpose, to enter on the premises of any person in order to inspect those premises or anything thereon for the purpose of any tax, rate or due or in order to carry out work connected with any property or installation which is lawfully on those premises and which belongs to that Government, that authority, or that body corporate, as the case may be; or

(*d*) that authorises, for the purpose of enforcing a judgment or order of a court, the search of any person or property by order of a court or entry upon any premises by such order, or that is necessary for the purpose of preventing or detecting criminal offences, and except so far as that provision or, as the case may be, the thing done under the authority thereof is shown not to be reasonably justifiable in a democratic society.".

Moreover, the European Convention Act, Chapter 317 of the Laws of Malta, (see Document 12) incorporates into Maltese Law the European Convention on Human Rights and Fundamental Freedoms, including Article 8 thereof, which forms part and parcel of Maltese Law. Article 8 of the ECHR is included in the First Schedule to the European Convention Act. Article 3(1) and (2) of the European Convention Act provide that:

"**3.** (1) The Human Rights and Fundamental Freedoms shall be, and be enforceable as, part of the Law of Malta.

(2) Where any ordinary law is inconsistent with the Human Rights and Fundamental Freedoms, the said Human Rights and Fundamental Freedoms shall prevail, and such ordinary law, shall, to the extent of the inconsistency, be void."

The Constitution of Malta also contains a provision on freedom of expression – see article 41 of the Constitution – and a provision of the protection of freedom of conscience and worship – see article 40 of the Constitution. On the other hand, the European Convention Act makes Articles 9 and 10 of the European Convention of

Human Rights part and parcel of Maltese Law directly enforceable in a Maltese court of law.

Freedom of information is regulated by the Freedom of Information Act,[23] Chapter 496 of the Laws of Malta (not all the provisions of this law have been brought into force), the Press Act,[24] Chapter 248 of the Laws of Malta, the Broadcasting Act,[25] Chapter 350 of the Laws of Malta, and the Data Protection Act – see article 6 regarding freedom of expression – and the Malta Communications Authority Act[26] – see article 4 regarding freedom of communication, right to privacy, disclosure of information received in confidence and maintenance of the authority of the judiciary.

Telecommunications content is defined in regulation 2(2) of the Electronic Communications (Personal Data and Protection of Privacy) Regulations – SL 399. 25 – as 'any information exchanged or transmitted between a finite number of parties by means of a publicly available electronic communications service. This does not include any information conveyed as part of a broadcasting service to the public over a public communications network except to the extent that the information can be related to the identifiable subscriber or user receiving the information'. Traffic and location data fall under the said expression and are protected in the same way as other forms of communications. All forms of communications can be retained for specific reason, that is, 'for the purpose of the investigation, detection or prosecution of serious crime' (regulation 19(1) of SL 440.01). In fact, regulation 4A of SL 399.25 provides as follows:

'4A. It shall be the obligation of a service provider to ensure that it has in place the necessary technical and administrative capacity and all other requirements to enable it to comply with the provisions of regulations 19 and 21 of the Processing of Personal Data (Electronic Communications Sector) Regulations, for the purposes of granting access to data as established in regulation 20 of the said regulations and to retain such data for such periods as established by regulation 22(*a*) and (*b*) of the said regulations.'

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

Article 41(2) of the Constitution and Article 10(2) of the ECHR provide a list of cases where freedom of expression may be restricted but the restriction has to be prescribed by law, made in terms of a legitimate aim and reasonably justifiable or necessary in a democratic society. The same applies with regard to Article 38(2) of the Constitution and Article 8(2) of the Convention with regard to privacy and

[23] See Document 13.

[24] See Document 14.

[25] See Document 15.

[26] See Document 16.

article 40(2) of the Constitution and Article 9(2) of the Convention with regard to freedom of worship.

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 such ruling has been made on the constitutionality/legality of the regulations transposing the Directive.

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

As such constitutional law has no provisions as mentioned above. So this task falls upon the Constitutional Court to determine. In doing so, the Constitutional Court will carry out an assessment/balance of interests in each individual case in order to establish what is reasonable justifiable or necessary[27] in a democratic society in terms of the human rights and fundamental provisions as contained in Chapter 4 of the Constitution of Malta and the European Convention Act which incorporates the European Convention on Human Rights into Maltese Law.

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)?

Neither the Constitution of Malta nor the European Convention Act contain any provisions to this effect. However, the Data Protection (Processing of Personal Data in the Police Sector) Regulations S.L. 440.05 allow the processing of personal data for historical, statistical or scientific purposes.

[27] There are no general limitations to any law interfering with a fundamental right as defined by the Constitution or the European Convention Act as each human right and fundamental freedom has its own limitations. These limitations are applied alternatively (meaning that any interference of a law with a human right or a fundamental freedom would have to be *either* reasonable *or* justifiable *or* necessary) and not cumulatively (meaning that all three preconditions would have to be fulfilled.

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?

I do not consider the retention obligation as restricting any fundamental right once its exercise is regulated by law and is reasonably justifiable or necessary in a democratic society. The only difficulty I see however is that whilst the service provider has to retain the data for a specified period, in the case of the Police and the Security Service there is no body which oversees that when such data is no longer needed it is destroyed.

The Data Protection Commissioner does have powers over the controller when the latter is processing personal data for police purposes but not over the Police and Security Service. In fact, regulation 4 of the Data Protection (Processing of Personal Data in the Police Sector) Regulations – SL 440.05) stipulates that:

'**4.** (1) Without prejudice to article 23 of the Act, the controller shall notify the Commissioner for Data Protection where in the exercise of his duty, the controller is required to process personal data for police purposes.

(2) The notification referred to in subregulation (1) must specify:

(*a*) the name and address of the controller and of any other person authorised by him in that behalf, if any;

(*b*) the purpose or purposes of processing;

(*c*) a description of the category or categories of data subject and of the data or categories of data relating to him;

(*d*) the recipient or categories of recipients to whom the data might be disclosed.'

The Data Protection Commissioner cannot control the Police and Security Services as in doing so he would be in breach of article 23 of the Data Protection Act which is transposing into national the Data Protection Directive. The exceptions on public security and national security are recognised by the European Convention on Human Rights, the human rights provisions in the Constitution and the case law of the European Court of Human Rights. Whether the lack of a provision in national law of the Commissioner supervising the Police and the Security Service at destroying data which is no longer in use would be considered as unreasonable, unjustifiable or unnecessary in a democratic society is a moot point. I very much

doubt that the European Court would rule this to be unjustifiable, etc. in a democratic society. Where public security and national security are concerned, Member States are given a wide margin of appreciation and the European Court's supervisory powers are exercised cautiously. But I see nothing wrong in the addition of a Protocol to the ECHR on the lines that there should be a mechanism introduced whereby data no longer in use by the Police and Security Service is destroyed within a prescribed time under the supervision of the Data Protection Commission in the case of Malta and equivalent public authorities abroad.

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

The law enforcement agencies are the Police and the Security Service. The data which they retain is that which they are empowered to retain by law. If they retain data which they are not allowed to retain, they would be in breach of the law. On the other hand, both these bodies have the right to request data from service providers. However, service providers are not involved as such in law enforcement: their duty is to pass on to the Police and Security Service that data[28] which these two governmental bodies are allowed to receive from service providers.

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

No constitutional law makes provision to the effect that costs are to be borne by service providers.

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?

International treaties need to be incorporated into Maltese Law to be effective. This is because Malta is a dualist state. The same applies to Council of Europe Conventions. With regard to the European Convention on Human Rights, the Convention have been incorporated into Maltese Law and is enforced by Maltese

[28] Although regulation 19 of SL 440.01 obliges service providers to provide the Police and Security Service with access to data, that the data provided has to be provided without undue delay and,in an intelligible form and in such a way that it is visible and legible, these regulations do not impose any duty on service providers to assist the Police and Security Services further. However, the Police can always, in terms of the Criminal Code, summon a service provider to give evidence in a court of law. I would understand that in such circumstances the court can dispense the service provider from his duty to confidentiality in the best interests of the due administration of justice. In so far as criminal court proceedings are concerned, there is a legal duty of assisting the court in the administration of justice irrespective of where the service provider gets paid or not.

Courts. The European Convention Act (which incorporates the ECHR into Maltese Law) is superior to all other laws in Malta except for the Constitution which is the supreme law of the land and the European Union Act which is on the same level of the European Convention Act. All the other laws obtaining in Malta are inferior to the Constitution which ranks first and the European Convention Act and the European Union Act[29] which rank second. Then all primary laws rank third and all subsidiary laws rank fourth. The European Union Act is the law through which Malta became and continues to be a member state of the European Union and regulates the reception of E.U. Law into Maltese Law.

The European Convention Act and the European Union Act rank second after the Constitution of Malta. Then all the other laws enacted by Parliament rank third. All these laws which rank third are not categorized amongst themselves hierarchically. So if one law in the third category runs counter to the Constitution, the European Convention Act and the European Union Act, it is these three laws which prevail over any law in the third category. There are approximately 500 such laws. But if a law in the third category runs counter to another law in the third category, Maltese Law does not state which law has precedence over the other in the same third category. However, one would probably apply the Roman Law principle that the last law enacted will supersede the previous law (quod postremum populus iussisset, id ius ratumque esset). Hence national laws incorporating international treaties rank in this third category (with the exception, of course, of the European Convention of Human Rights and Fundamental Freedoms and the EU Treaty).

With regard to S.L. 440.05 - Data Protection (Processing of Personal Data in the Police Sector) Regulations – the expression 'Police' includes also the Security Services. See the definitions of "for Police Purposes" and "controller" in regulation 2(1) of SL 440.05 which apply also to the Security Service. So SL 440.05 although referring to the "Police Sector" in fact includes also the Security Service. This is because in Malta the Security Service is manned by Police Officers and the Head of the Security Service is a Police Officer. The distinction between the Police and the Security Service is very blurred. Moreover, the Security Service operates from Police General Headquarters.

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?

Directives have to be transposed in order to become law from a national law point of view. A directive can be transposed either in an act of parliament or in a subsidiary law. If this process does not take place, the directive is not law from a national law point of view.

[29] See Document 17.

However, the European Court of Justice's jurisdiction on the direct effects of a directive are observed in the national legal context, that is, the effect that a Directive may grant a certain right to an individual if certain conditions, as set out by the ECJ e.g. in the case C-26/62 (Van Gend), are fulfilled. Article 5 of the European Union Act (Chapter 460) provides that:

'5.(1) For the purposes of any proceedings before any court or other adjudicating authority, any question as to the meaning or effect of the Treaty, or as to the validity, meaning or effect of any instruments arising therefrom or thereunder, shall be treated as a question of law and if not referred to the Court of Justice of the European Communities, be for determination as such in accordance with the principles laid down by, and any relevant decision of, the Court of Justice of the European Communities or any court attached thereto.

(2) Judicial notice shall be taken of the Treaty, of the Official Journal of the European Union and of any decision of, or expression of opinion by, the Court of Justice of the European Communities or any court attached thereto on any such question as aforesaid, and the Official Journal shall be admissible as evidence of any instrument or any other act thereby communicated of any of the Communities or of any institution of the European Union.'

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?

Yes, the Ratification of Treaties Act, Chapter 304 of the Laws of Malta,[30] does not allow Malta to transfer national sovereignties to the European Union unless and until the procedure prescribed in that law are followed. Hence a new E.U. treaty or an amendment to the existing treaty would require Parliamentary approval.

Article 65 of the Constitution provides that all laws made by Parliament – including the Constitution itself – have to comply with EU Law. It reads as follows:

'65. (1) Subject to the provisions of this Constitution, Parliament may make laws for the peace, order and good government of Malta in conformity with full respect for human rights, generally accepted principles of international law and Malta's international and regional obligations in particular those assumed by the treaty of accession to the European Union signed in Athens on the 16th April, 2003.'

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

[30] See Document 18.

authorities of these entities and between these authorities and the authorities of the central state/federal state?

Data retention powers are exercised by the Police and the Security Service. No regional territorial entities are vested with any such powers or have competence in so far as data retention is concerned. Malta is a unitary not a federal state.

The ministry responsible for the Malta Police Force and the Security Services is the Ministry for Justice and Home Affairs. The Prime Minister does retain certain functions under the Security Services Act with regard to the Security Services. The courts retain a judicial supervision over the Police and Security Service. In the case of the Police there is established under the Police Act a Police ombudsman known as the Police Board, and in the case of the Security Service there is established under the Security Services Act a Security ombudsman known as the Security Commissioner.

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

Apart from what has been stated in reply to question 44, neither the Constitution nor the European Convention Act set any limits regarding the transmission of retained data to other countries.

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?

First, it has to be noted that the law as it obtains considers data retention as an exception rather than the rule and, where it is allowed, it is permitted for a brief period of time and with regard to certain well defined categories of information. Moreover, the entities which have access to such data are few in number – two as a matter of fact – and they are also regulated in the way they manage this data. So, in this respect, it can safely be stated that there are adequate safeguards in this respect.

As to suggestions for improvement, I think that the following measures should be adopted:

- although the Police and the Security Service are bound to destroy data which is no longer needed, the law does not oblige a mandatory overseeing mechanism to oversee the actual destruction. Hence it is recommended that when such data is destroyed a report is submitted to the Data Protection Commission of such destruction and when the destruction takes place the Data Protection Commissioner or his delegate is present to evidence the destruction.

- the Police and the Security Service should, at annual intervals, report to the Data Protection Commission which data they are retaining so that he may have

an inventory of such data and be in a better position to exercise his supervisory role over the Police and the Security Service.

- There should be a legal requirement on the Data Protection Commissioner to compile and publish statistics as to the amount, frequency and category of requests for data retention made by the Police and the Security Service to service providers.

- The law should prescribe the form of the technical and administrative capacity which service providers should comply with.

- The law should prescribe the types of measures which are to be applied by service providers to ensure that the technical and administrative capacity referred to above is effectively complied with.

- Technical standards to be applied with respect to data retention and transmission should be prescribed by law.

- The procedure of data transmission from the retaining to the accessing party should be prescribed by law.

- Generally, more information should be released in the public domain with regard to the implementation of the directive. Service providers and accessing parties should be required to submit an annual report to the Data Protection Commissioner so that he can publish such information in his annual report.

- More information needs to be published by the Data Protection Commissioner as to the supervisory control which he exercises in terms of the directive such as how many times has he carried out an inspection of the data retained by the accessing parties, what where his findings, where any infringements of the directive found, were these infringements complied with within a reasonable time, etc.

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

Malta

Professor Kevin Aquilina

Part 2: Overarching issues and country-specific questions

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

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

The Constitution of Malta provides for freedom of expression in article 41 and the European Convention Act, Chapter 319 of the Laws of Malta, incorporates into Maltese Law the European Convention on Human Rights and Fundamental Freedoms, including Article 10 on freedom of expression. National constitutional law does not however specifically provide for a right to communicate anonymously. Nor do these two provisions prohibit anonymous communications. On the contrary, there is no general law in Malta which disallows anonymous communications. That said, nevertheless, anonymous communication might still be in breach of criminal law (e.g. obscenity, blasphemy, libel, etc.). In the latter case, if the anonymity is revealed such person can be the subject of criminal proceedings. If the anonymity is not revealed, then it is the Editor of the medium concerned who accepts responsibility for whatever an anonymous person writes or publishes in his newspaper, broadcast, blog, etc.

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

   At the moment of writing there are no amendments being proposed to current data retention legislation in Malta. Nor is any discussion taking place on data retention or on the quick freeze option.

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?**

   Private actors have a duty to provide to government authorities certain information which is of a private nature by means other than data retention, to co-operate with public authorities in the detection, investigation and prosecution of criminal offences and for any other of the legitimate purposes for which providers are also obliged to retain data. Examples of disclosure of information required by law include the following instances:

   (a) *notification/reporting of cases of disease*: it is the duty of a medical practitioner to report any cases of disease that can be considered a public health risk, even if this conflicts with the right of privacy of the individual patient. The following are specifically mentioned in legislation:

   (i) notifiable diseases, including food poisoning. The list of notifiable diseases is issued by the Superintendent of Public Health in terms of article 27 of the Public Health Act, Chapter 465 of the Laws of Malta;

   (ii) the Notification of Cancer Act, Chapter 154 of the Laws of Malta, article 3, provides that a 'medical practitioner attending on or called in to visit a patient shall forthwith, on becoming aware that the patient is suffering from cancer in any form, send to the Superintendent of Public Health a certificate stating the name, age, occupation and address of the patient and the type of cancer from which, in his opinion, the patient is suffering as well as the organ, tissue or site which is affected by the disease.';

   (iii) veneral diseases also have to be reported by doctors in terms of article 3 of the Venereal Diseases (Treatment) Act, Chapter 124 of the Laws of Malta;

(iv) the registration of drug addicts with the Superintendent of Public Health is covered by subsidiary legislation, Registration of Drug Addicts Regulations, SL 31.21, regulation 3(1);

(b) retention of personal data concerning criminal offences:

(i) the Conduct Certificates Ordinance, Chapter 77 of the Laws of Malta, allows the Police to retain data concerning a person's criminal conduct;

(ii) the registration of sexual offenders and other offenders who commit offences of serious violence (this is still a Bill not a law).

(c) duty to report in the case of offences related to the safety of the state:

(i) article 61 of the Criminal Code, Chapter 9 of the Laws of Malta, reads as follows:

'61. Whosoever, knowing that any of the crimes referred to in the preceding articles of this Title [Crimes against the Safety of the Government] is about to be committed, shall not, within twenty-four hours, disclose to the Government or to the authorities of the Government, the circumstances which may have come to his knowledge, shall, for the mere omission, be liable, on conviction, to imprisonment for a term from nine to eighteen months.'

(ii) article 22 of the Official Secrets Act, Chapter 50 of the Laws of Malta, reads as follows:

'22. It shall be the duty of every person to give on demand to any Police officer not below the rank of inspector appointed by the Commissioner of Police for the purpose, or to any member of the armed forces of Malta engaged on guard, sentry, patrol, or other similar duty, any information in his power relating to an offence or suspected offence under this Act, and, if so required, and upon tender of his reasonable expenses, to attend at such time and place as may be specified for the purpose of furnishing such information, and if any person fails to give any such information or to attend as aforesaid, he shall be liable, on conviction, to imprisonment for a term not exceeding two years or to a fine (*multa*) or to both such imprisonment and fine.'

(d) *duty to grant access to information in the case of Money Laundering:* article 4 of the Prevention of Money Laundering Act, Chapter 373 of the Laws of Malta, empowers the Criminal Court to order any person to grant access to information with regard to money laundering investigations.

(e) *when professional secrecy is done away with*: article 6A of the Professional Secrecy Act, Chapter 377 of the Laws of Malta, sets out the cases where a member of a profession is dispensed of professional secrecy.

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 rules governing the rights of persons to refuse to testify/to deliver evidence against themselves are found in the following laws:

   the *Constitution of Malta* in article 39(10) provides that: 'No person who is tried for a criminal offence shall be compelled to give evidence at his trial.' It further provides in article 39(5) that 'Every person who is charged with a criminal offence shall be presumed to be innocent until he is proved or pleaded guilty.'

   the *European Convention Act*: Article 6 of the European Convention Act dealing with the right to a fair hearing in a criminal trial has been interpreted by the European Court of Human Rights to include the right against self-incrimination (see, for instance, Funke v. France (A 256-A 1993). This provision forms part of the Laws of Malta in terms of the European Convention Act.

   the *Criminal Code*: Article 643 of the Criminal Code provides that: 'No witness may be compelled to answer any question which tends to expose him to any criminal prosecution'. Article 642 further provides that:

   '**642**. (1) Advocates and legal procurators may not be compelled to depose with regard to circumstances knowledge whereof is derived from the professional confidence which the parties themselves shall have placed in their assistance or advice.

   (2) The same rule shall apply in regard to those persons who are by law bound to secrecy respecting circumstances on which evidence is required.'

   the *Code of Organization and Civil Procedure, Chapter 12 of the Laws of Malta*: Article 589 provides that: '**589.** A witness cannot be compelled to answer any question the answer to which may subject him to a criminal prosecution'. Article 588 further provides that:

   '**588**. (1) No advocate or legal procurator without the consent of the client, and no clergyman without the consent of the person making the confession, may be questioned on such circumstances as may have been stated by the client to the advocate or legal procurator in professional confidence in reference to the cause, or as may have come to the knowledge of the clergyman under the seal of confession or loco confessionis.

(2) Unless by order of the court, no accountant, medical practitioner or social worker, psychologist or marriage counselor may be questioned on such circumstances as may have been stated by the client to the said person in professional confidence or as may have come to his knowledge in his professional capacity.

(3) This privilege extends to the interpreter who may have been employed in connection with such confidential communications.'

(e) the Code of Ethics & Conduct for Advocates provides as follows:

'Chapter VI: Confidentiality

Rule 1

Besides being bound by professional secrecy, an advocate is under a duty to keep confidential the affairs of clients and to ensure that his or her staff do the same.

Rule 2

The duty to keep confidential information about a client and his or her affairs applies irrespective of the source of the information.

Rule 3

The duty to keep confidential a client's business continues until the client permits disclosure or waives the confidentiality.

Rule 4

The duty to keep a client's matters confidential, as opposed to what applies to the duty of professional secrecy, can be overridden in certain exceptional circumstances and shall include those cases in which an advocate is required to disclose confidential information in terms of law; and those cases in which such disclosure is essential for an advocate to defend himself in any proceedings taken against him by or on the complaint of a client or a former client in which event the disclosure shall be limited to what is indispensable for the advocate to defend himself.

Rule 5

An advocate must not disclose a client's address when expressly prohibited from so doing by his client or when he has reasonable grounds to assume that such disclosure would be prejudicial to his client.

Rule 6

An advocate must not make any profit by the use of confidential information obtained in the exercise of his or her profession for his or her own purposes or the purposes of third parties.'

As these rules cover evidence in general, they include 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.

These rights to refuse to testify do conflict with data retention in a way that they bar these data from being used as an evidence in court in those cases where such use might incriminate the person giving evidence.

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

The law does not state where and how are data requested by entitled bodies to be stored by these bodies once obtained. However, regulation 19(2) of the Processing of Personal Data (Electronic Communications Sector) Regulations, S.L. 440.01, obliges service providers to provide the Police or the Security Service (the two Government bodies entitled by law to have access to data and to retain it) to provide such data 'in an intelligible form and in such a way that it is visible and legible'. The law does not state however how do the Police and Security Service store such data, e.g. it is stored as a hard copy; it is inputted in a computer programme; etc.

The two entitled bodies (Police and Security Service) have to take security measures relating to processing in terms of regulation 14 of the Data Protection (Processing of Personal Data in The Police Sector) Regulations, S.L. 440.05 on the following lines:

'**14.** (1) The controller shall implement appropriate technical and organisational measures to protect the personal data that are processed against accidental destruction or loss or unlawful forms of processing thereby providing an adequate level of security that gives rise to the:

technical possibilities available;

cost of implementing the security measures;

special risks that exist in the processing of personal data;

sensitivity of the personal data being processed.

(2) Where the controller engages a processor, the controller shall ensure that the processor:

(a) can implement the security measures that must be taken;

(b) actually takes the measures so identified by the controller.'

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.**

I am not aware of any published statistics as referred to in question 6 even though regulation 24 of the Processing of Personal Data (Electronic Communications Sector) Regulations, S.L. 440.01, provides that:

'**24.** (1) Service providers shall, in relation to the retention of data under this Part, provide on an annual basis, the following information to the Data Protection Commissioner:

(a) the cases in which information was provided under this Part;

(b) the time elapsed between the date on which the data were retained and the date on which the transmission of the data was requested;

(c) any cases where requests for data could not have been met.

(2) Any statistics provided under this regulation shall not contain any personal data.'

There is no requirement, in the above regulation, to oblige the Information and Data Protection Commissioner to publish the statistics he receives.

B. Country-specific questions

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

I do not think that retention of data for an indefinite period of time satisfies the test of proportionality as applied by the European Court of Human Rights. Nor do I consider there to be a pressing social need to retain such data indefinitely or for an unreasonable period of time. On the contrary, I think that criteria should be developed to ensure that data is not retained beyond what is reasonable and necessary in a democratic society. Data should no longer be retained in the following circumstances:

(a) when the person being investigated by the Police dies;

(b) when a person charged before a court of criminal justice dies during the pendency of the proceedings;

(c) when the criminal offence in terms of which a person may be accused before a court of criminal justice becomes time-barred and, therefore, no criminal action may be prosecuted before a court of criminal justice;

(d) when there is a definitive judgment in favour or against the accused which has become res judicata. Any data retained by the Police following the judgment becoming res judicata should be destroyed;

(e) when a court of criminal jurisdiction has declared that evidence produced in court has been taken in violation of a law (e.g. the accused was, during police interrogation tortured and made to sign a statement that he has committed all the crimes listed in that statement. Such statement which will also provide the details of the accused and other private information should be destroyed. The same happens where the Police have framed up a person by elevating his fingerprints/DNA and placed them at the scene of the crime giving the impression that the accused has actually committed the offence when they know that this is not the case);

(f) when the evidence has been filed in court and therefore there is no need to retain copies thereof, especially where the court orders the destruction of such evidence or that it be handed over to the accused;

(g) when a criminal or administrative investigation has concluded that there is no prima facie case against the accused for the institution of criminal/administrative proceedings.

I also think that when data is retained for more than two years, there should be a review mechanism to authorise the retention of such data beyond the said two year period. I do not exclude the possibility that an extension may be provided for a further two year period and, if need, be, for subsequent two year periods. However, the competent authority must make a case to justify why the data should be retained for a further period/s. The Freedom and Data Protection Commissioner or a court of law should be tasked with this review procedure.

8. 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.

There are two main interests to be balanced: privacy on the one hand and public order on the other. By public order I here mean the detection and investigation of crime by the competent authorities. Whilst privacy is not an absolute right and hence limitations and restrictions to this right are allowed by Human Rights Law, these restrictions and limitations should not become the rule thereby negating privacy. So whilst privacy may be restricted and limited, this has to be done by observing certain criteria. To retain data indefinitely is not considered to be proportionate because there might arise a number of situations where the retention of that data might no longer be required. For instance, if a court of criminal jurisdiction has declared that blood samples were taken by the police in breach of one's right to privacy, then those samples cannot be retained by the courts, nor by the Police should they still have under their custody other such samples. The rule of law requires that in such cases the Police have to follow and apply any directions which the court may give in relation to those samples. For the police to continue to

retain such samples, notwithstanding a court pronouncement ordering their destruction, would breach the rule of law and be in contempt of the authority of the court. Such police action would not be proportional because there is surely no pressing social need to retain such blood samples.

9. **As regards your answer to question 60 of the first questionnaire (limits to the conferral of powers to the EU/to the applicability of EU law in Malta): Are there any limits as to the *subject matter*, e.g. that EU law may not be contrary to certain essential provisions laid down in the Constitution (e.g. core fundamental rights)?**

Article 6 of the Constitution of Malta states that:

'**6.** Subject to the provisions of sub-articles (7) and (9) of article 47 [referring to the interpretation of the Constitution] and of article 66 of this Constitution [referring to the procedure for alteration of the Constitution], if any other law is inconsistent with this Constitution, this Constitution shall prevail and the other law shall, to the extent of the inconsistency, be void.'

On the other hand, article 65(1) of the Constitution states that:

'**65.** (1) Subject to the provisions of this Constitution, Parliament may make laws for the peace, order and good government of Malta in conformity with full respect for human rights, generally accepted principles of international law and Malta's international and regional obligations in particular those assumed by the treaty of accession to the European Union signed in Athens on the 16th April, 2003.'

From a reading of these two provisions, the following can be stated:

the European Union Act, Chapter 460 of the Laws of Malta, is an ordinary law and hence subject to the Constitution of Malta's article 6. This Act was enacted to provide for Malta's accession to the European Union and for Malta to be in a position to receive European union Law within its municipal law. If an inconsistency exists between the Constitution of Malta and Maltese Law transposing EU law or EU law which is directly applicable in Malta, it is the Constitution of Malta which prevails, even if this interpretation of Maltese Law might bring domestic law in breach of E.U. Law;

on the other hand, in terms of article 65(1) of the Constitution, Parliament has to make municipal laws which are 'in conformity' with the treaty of EU accession. So if this always happens, then there can be no conflict between Maltese municipal law and EU law but if there are extant provisions in the Constitution which run counter to EU Law or if new provisions are added to the Constitution of Malta which do not comply with European Union Law, then there is a problem here because from the point of view of domestic Constitutional Law, it is the Constitution which prevails but from the point of view of public international law, it is EU Law which prevails. According to the Vienna Convention on the Law of Treaties 1969, Article 27, 'A

party may not invoke the provisions of its internal law as justification for its failure to perform a treaty.'

The current legal provision needs to be addressed to ensure that if there is a conflict between EU Law and the Constitution of Malta it is the former (not the latter as is the position to date) which prevails. Therefore, to date, the position is that if EU Law is contrary to the Constitution of Malta then Maltese not EU Law prevails. Naturally, there is nothing to stop Parliament, on a case to case basis, to amend the Constitution of Malta each time a problem arises to bring it in line with EU Law.

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

According to regulation 18(1) of the Processing of Personal Data (Electronic Communications Sector) Regulations, S.L. 440.01, 'a service provider of public available electronic communications services or of a public communications network shall retain the data specified in regulation 20 [which sets out the categories of data to be retained] to the extent that those data are generated or processed by such providers in the process of supplying the communications services concerned.'

This means that the obligation to retain data falls on either a service provider of publicly available electronic communications services or a service provider of a public communications network to retain the data and not on both of them concurrently. In order to determine which one of these two service providers is obliged to retain the said data, the criterion to be used is that of establishing which of these two service providers has 'generated or processed' data 'in the process of supplying the communications services concerned'. The regulation does not therefore require data to be retained more than once but requires the applicable service provider – who can be the network operator or the service provider, as the case may be – to retain such data. This regulation therefore prevents the same traffic/location data from being retained more than once. The regulation does not stipulate the procedure to be adopted by both service providers to establish who should retain the data or which procedure is to be applied should they disagree as to who should retain such data.

11. **As regards your answer to question 39 of the first questionnaire: Does Maltese law provide for rules on the transfer of personal data to third countries that correctly transpose the provisions laid down in Chapter IV of Directive 95/46/EC? If so, please indicate the relevant legal norms.**

In so far as transfer of personal data to third countries is concerned, the Third Country (Data Protection) Regulations, S.L. 440.03, define in regulation 4 a third country as 'any country that at the relevant time is not a Member State of the European Union.' It then obliges in regulation 5 data controllers to notify the

Commission of any transfer of personal data resulting from a processing operation to a third country, that is, a non-E.U. country.

As such there is no rule in Maltese Law that provides for rules on the transfer of personal data to third countries that correctly transpose the provisions laid down in Chapter IV of Directive 95/46/EC. However, the Data Protection Act in article 27 empowers the Information and Data Protection Commissioner to determine whether the third country to which the data is to be transferred enjoys an adequate level of protection on the lines of Chapter IV of Directive 95/46/EC:

'27. (1) Without prejudice to the provisions of article 28, the transfer to a third country of personal data that is undergoing processing or intended processing, may only take place subject to the provisions of this Act and provided that the third country to which the data is transferred ensures an adequate level of protection.

(2) The adequacy of the level of protection of a third country shall be assessed in the light of all the circumstances surrounding a data transfer operation or a set of data transfer operations; particular consideration shall be given to the nature of the data, the purpose and duration of the proposed processing operation or operations, the country of origin and country of final destination, the rules of law, both general and sectoral, in force in the third country in question and the professional rules and security measures which are complied with in that country.

(3) It is for the Commissioner to decide whether a third country ensures an adequate level of protection.

(4) The transfer of personal data to a third country that does not ensure adequate protection is prohibited.'

Not only does Maltese Law not require third countries to whom it might transfer data to have transposed within their municipal law the provisions laid down in Chapter 4 of Directive 95/46/EC but it allows the Minister to transfer personal data to third countries without being restricted on the grounds of protection of privacy:

'28. (1) For the purpose of implementing any international convention to which Malta is a party or any other international obligation of Malta, the Minister may by Order designate that the transfer of personal data to any country listed in the said Order shall not, notwithstanding the provisions of this Act or any other law, be restricted on grounds of protection of privacy. In making such Order the Minister may include conditions and restrictions provided for in any said international instrument.

(2) A transfer of personal data to a third country that does not ensure an adequate level of protection within the meaning of article 27(2) may be effected by the controller if the data subject has given his unambiguous consent to the proposed transfer or if the transfer -

(*a*) is necessary for the performance of a contract between the data subject and the controller or the implementation of precontractual measures taken in response to the data subject's request;

(*b*) is necessary for the performance or conclusion of a contract concluded or to be concluded in the interests of the data subject between the controller and a third party;

(*c*) is necessary or legally required on public interest grounds, or for the establishment, exercise or defence of legal claims;

(*d*) is necessary in order to protect the vital interests of the data subject; or

(*e*) is made from a register that according to laws or regulations is intended to provide information to the public and which is open to consultation either by the public in general or by any person who can demonstrate legitimate interest, provided that the conditions laid down in law for consultation are fulfilled in the particular case.

(3) Without prejudice to subarticle (1) the Commissioner may authorise a transfer or a set of transfers of personal data to a third country that does not ensure an adequate level of protection within the meaning of article 27(2):

Provided that the controller provides adequate safeguards, which may result particularly by means of appropriate contractual provisions, with respect to the protection of the privacy and fundamental rights and freedoms of individuals and with respect to their exercise.'

Are the technical and organisational measures necessary to implement the legal requirements on data security (as far as I understand from your answers to questions 21, 26 and 40 of the first questionnaire, the only provisions in this respect are Regulation 23 of S.L. 440.01, Regulation 14 of S.L. 440.05 and Regulation 4A of S.L. 399.25) standardised or specified any further, e.g. through guidelines issued by the supervisory authority)? If so: Are these specifications binding or not for the bodies concerned? Please describe their content.

There are no further technical and organisational measures necessary to implement the legal requirements on data security apart from those specified in the question above. Nor are there any specifications which have been published, even if by way of guidelines or non-binding status.

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

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

b) **secure data storage: cryptographic security (e.g. general obligation to encrypt the data retained, possibly further detailed by specifications e.g. on the encryption algorithm to be used or on the safe custody of the crypto-keys)**

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

d) **access logging**

e) **secure (irreversible) deletion after expiry**

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

g) **secure data transmission (cryptographic security, postal delivery)**

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

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

j) **staff training/internal control mechanisms to ensure compliance with the law and other rules**

k) **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)**

This is not the case.

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

No such measures described above exist.

14. **Which public bodies are responsible for supervising that the data retention rules (other than the rules on data protection which are under the supervision of the Information and Data Protection Commissioner) are implemented correctly by the obligated parties (network operators, service providers)?**

It is the Information and Data Protection Commission who supervises the obligated parties (network operators, service providers). The said Information and Data Protection Commissioner is independent of Government. Article 37(1) of the Data Protection Act provides that:

‘37. (1) In the exercise of his functions under this Act the Commissioner shall act independently and shall not be subject to the direction or control of any other person or authority.’

Article 40 of the Data Protection Act lists the following amongst the functions of the Information and Data Protection Commissioner:

‘(b) to exercise control and, either of his own motion or at the request of a data subject, verify whether the processing is carried on in accordance with the provisions of this Act or regulations made thereunder;

(*c*) to instruct the processor and controller to take such measures as may be necessary to ensure that the processing is in accordance with this Act or regulations made thereunder;

(*d*) to receive reports and claims from data subjects or associations representing them on violations of this Act or regulations made thereunder, to take such remedial action as he deems necessary or as may be prescribed under this Act, and to inform such data subjects or associations of the outcome;

(*e*) to issue such directions as may be required of him for the purposes of this Act;

(*f*) to institute civil legal proceedings in cases where the provisions of this Act have been or are about to be violated and to refer to the competent public authority any criminal offence encountered in the course of or by reason of his functions;’

…

‘(i) to order the blocking, erasure or destruction of data, to impose a temporary or definitive ban on processing, or to warn or admonish the controller;’

…

‘(*l*) at the request of a data subject to verify that the processing of the personal data described in article 23 of this Act is compliant with the provisions of this Act or of any law as specified in subarticle (1) of the said article 23 and in such a case the data subject shall be informed accordingly.’

There is the possibility to appeal from the Commissioner’s decision to the Information and Data Protection Appeals Tribunal in terms of article 49 of the Data Protection Act. This is also a further appeal on a question of law from the Tribunal’s decision to the Court of Appeal in terms of article 51 of the Data Protection Act.

Regulation 16 of the Processing of Personal Data (Electronic Communications Sector) S.L. 440.01 further confirms that it is the Information and Data Protection Commissioner who is entrusted with law enforcement:

'**16.** Where it is alleged that any of these regulations have been contravened, the Authority [the Malta Communications Authority] or any aggrieved person may request the Commissioner to exercise his enforcement functions in respect of that contravention: Provided that nothing in this regulation shall be interpreted as a limitation on the discretionary powers of the Commissioner.'

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

It is the Information and Data Protection Commission who supervises the bodies entitled to obtain access to the data retained (Police and Security Service). The said Information and Data Protection Commissioner is independent of Government. Article 37(1) of the Data Protection Act provides that:

'37. (1) In the exercise of his functions under this Act the Commissioner shall act independently and shall not be subject to the direction or control of any other person or authority.'

Article 40 of the Data Protection Act lists the following amongst the functions of the Information and Data Protection Commissioner:

'(b) to exercise control and, either of his own motion or at the request of a data subject, verify whether the processing is carried on in accordance with the provisions of this Act or regulations made thereunder;

(*c*) to instruct the processor and controller to take such measures as may be necessary to ensure that the processing is in accordance with this Act or regulations made thereunder;

(*d*) to receive reports and claims from data subjects or associations representing them on violations of this Act or regulations made thereunder, to take such remedial action as he deems necessary or as may be prescribed under this Act, and to inform such data subjects or associations of the outcome;

(*e*) to issue such directions as may be required of him for the purposes of this Act;

(*f*) to institute civil legal proceedings in cases where the provisions of this Act have been or are about to be violated and to refer to the competent public authority any criminal offence encountered in the course of or by reason of his functions;'

'(i) to order the blocking, erasure or destruction of data, to impose a temporary or definitive ban on processing, or to warn or admonish the controller;'

'(*l*) at the request of a data subject to verify that the processing of the personal data described in article 23 of this Act is compliant with the provisions of this Act or of

any law as specified in subarticle (1) of the said article 23 and in such a case the data subject shall be informed accordingly.'

There is the possibility to appeal from the Commissioner's decision to the Information and Data Protection Appeals Tribunal in terms of article 49 of the Data Protection Act. This is also a further appeal on a question of law from the Tribunal's decision to the Court of Appeal in terms of article 51 of the Data Protection Act.