Council of the
European Union

**Brussels, 15 June 2018**
**(OR. en)**

**12749/1/06**
**REV 1 DCL 1**

**SCH-EVAL 136**
**COMIX 748**

**DECLASSIFICATION**

| | |
|---|---|
| of document: | ST12749/1/06 REV 1 RESTREINT UE/EU RESTRICTED |
| dated: | 20 October 2006 |
| new status: | Public |
| Subject: | Schengen evaluation of the new Member States<br>- MALTA: Report on Data Protection |

Delegations will find attached the declassified version of the above document.

The text of this document is identical to the previous version.

COUNCIL OF
THE EUROPEAN UNION

Brussels, 20 October 2006

12749/1/06
REV 1

RESTREINT UE

SCH-EVAL 136
COMIX 748

**REPORT**

| | |
|---|---|
| from : | Data Protection Evaluation Committee |
| to: | Schengen Evaluation Working Party |
| Subject : | Schengen evaluation of the new Member States<br>- MALTA: Report on Data Protection |

According to the mandate given by the Decision of the Executive Committee of 16 September 1998 setting up a Standing Committee on the Evaluation and implementation of Schengen (SCH/Com-ex (98) 26 def) to the Schengen evaluation working group, a team of experts has visited Malta from 12 to 14 July 2006 according to the program mentioned in doc. 5014/4/06 REV 4 SCH-EVAL 1 COMIX 4.

The following experts participated:

FIN - Reijo Aarnio (Leading Expert)
B - Willem Debeuckelaere
CZ - Miroslava Matousova
D - Matthias Taube
EE - Urmas Kukk
GR - Maria Alikakou
I - Vanna Palumbo
LT – Vaida Linartaitė
SI - Klemen Dobrota
SK - Peter Lieskovsky
CION - André Rizzo
CS - Wouter van de Rijt



**PRELIMINARY REMARKS**

*The Malta Data Protection Authority and all the Ministries involved have considerably helped the work of the inspection team by providing in advance of the mission written information on the main issues, including the translation of the key legislation. The experts have valued the interest shown by the Commissioner himself and his staff by attending and by contributing in person and extensively to the evaluation work.*

*It should be noted that this evaluation, like the ones to follow in the new Member states, but unlike previous Schengen evaluation missions, are of a special nature: instead of verifying the practical implementation of the Schengen acquis, the evaluation team has been assessing the capacity and the capability of the Data Protection Authority (further DPA) to properly perform all its duties in relation to the implementation of the provisions on Data protection in the Schengen acquis.*

*It should be taken into account, that the new Member States apply the Schengen acquis category I (Articles 126 – 130 of the Schengen Convention) as of the date of accession to the EU.*

**Management summary**

Malta has shown that it has developed the appropriate legal framework for Data Protection, supplemented by an impressive set of implementing measures, like guidelines, written procedures, training and awareness sessions, which altogether rank as best practices among the Schengen partners.

From a technical point of view, experts noted that Malta is planning to establish well known technical solutions in the implementation phase of the NSIS and SIRENE system based on the experience of other Member states. The authorities are aware of possible problems. It is recommended to check after the finalisation of the SIS II legal instruments whether it is necessary to submit a special implementing law.



## 1. LEGAL BASE AND ORGANISATIONAL ENVIRONMENT FOR DATA PROTECTION

Data protection in Malta is based on the following instruments:

The Data Protection Act Cap. 440 (which transposes Dir 95/46/EC) of the Laws of Malta, as was the Convention 108 of the CoE

Subsidiary legislation under the DPA Act,

- Processing of Personal Data (Electronic Communications Sector) Regulations, LN 16 of 2003 as amended by L.N. 153 of 2003, L.N. 522 of 2004, and L.N. 109 of 2005
- Notification and fees (Data Protection Act) Regulations, L.N. 154 of 2003, as amended by L.N. 162 of 2004
- Third Country (Data Protection Act) Regulations, L.N. 155 of 2003
- Processing of Personal Data (Protection of minors) Regulations, L.N. 125 of 2004
- Data Protection (Processing of Personal Data in the Police Sector) Regulations, L.N. 142 of 2004.

Although the Act foresees in its article 5b that the Act does not apply to processing operations concerning public security, defence, state security and activities of the State in areas of criminal law, the Act enables the Minister responsible to enact regulations applicable to police law enforcement activities. Such regulations have been issued under the Police Sector Regulations which explicitly extend the applicability of the Act to the processing of data held by the Police, under the supervision of the Data Protection Commissioner, empowered with his competences deriving from the Data Protection Act.

Experts were told by the Commissioner that most of the provisions of Recommendation (87)15 of the Council of Europe were implemented in Malta through the Police Sector Regulations (LN142/04). Malta should however formalise the application of the entire Recommendation at short notice, since this has actually become an obligation under art. 129 of Schengen, which entered into force in Malta on 1 My 2004, together with the other so-called "Category I" measures of the Schengen acquis. [1]

Since the Maltese authorities told the experts that "the law is currently being studied to be practically re-written taking into consideration the International and EU obligations and data Protection Principles", experts recommend that this amendment be used to materialise the implementation of the said Recommendation.

The Maltese Data Protection Authority has published guidelines on a variety of issues, like processing of visual images in schools, good practices for the insurance business sector. Malta could consider publishing a manual explaining what does Schengen Acquis mean to Maltese population, including a chapter on Data protection.

It is worth mentioning as well that a Data Protection Implementation Unit has been established at the Office of the Prime Minister, and which is in charge of ensuring the proper implementation of the Data protection legislation in the ministries and other public bodies.



[1] Malta added that the remaining provisions of the Recommendation, which relate to retention periods, will be implemented by means of new ad-hoc legislation which will cover all aspects of offences of a criminal nature;

**The Office of the Data Protection Commissioner**

The Data Protection Commissioner (later in this report the DPA for Data Protection Authority), has been established in Malta by the Data Protection Act of 2002.

The Commissioner is appointed by the Prime Minister after consultation with the Leader of the Opposition. He can only be removed by a vote of the House of Representatives, supported by two-thirds of its members. Experts consider this to be a strong mark of independence.

The Commissioner is also independent in his competences as employer. He hires his own staff, within the limits granted by the budget. The budget is made up by 50 % of a subvention voted by the House of Representatives and for the remaining part by notification fees. Moreover, income from administrative fines shall also accrue to the Office. The DPA has granted itself a stabilising factor in this income by agreeing with the Ministry of Finance on a 3-years budget planning.

The DP Law requires from the Commissioner a statement of accounts in respect of each financial years, that is audited by auditor/s chosen by the Commissioner himself. The Auditor general of the State, on behalf of the Minister of finance, can play a supervisory role.

The statement of account is public and is presented jointly with the Annual Report.

Moreover , article 39 paragraphs 3, 4 of the Data Protection Act of Malta establishes provisions for the appointment of a temporary Commissioner.

The Commissioner shall have the following functions:

(a) to create and maintain a public register of all processing operations according to notifications submitted to him as specified in this Act;

(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;

(g) to encourage the drawing up of suitable codes of conduct by the various sectors affected by the provisions of this Act and to ascertain that the provisions of such codes are in accordance with the provisions of this Act (…).

The DPA is competent for both the private and public sector, including the police ( reference to the tasks assigned to the DPA under Regulation 142 of 2004). The DPA prepares and presents the Annual report publicly (Art. 40, lett.k).

The current number of staff is 11.

A new IT system has been introduced and several office tasks have been automated.

The DPA has officially been designated as the supervisory authority over the SIS. A Schengen national coordination committee has been set up in order to prepare, both legally and technically, Malta to the accession in Schengen and the DPA is participating in it.

## 2. DATA SUBJECT RIGHTS AND COMPLAINTS HANDLING

### The right of access

Individuals have a direct right of access about the processing of their personal data. The data controller is committed to giving that information without excessive delay, although there is no fixed term for that. The data controller should not necessarily give physical copies but written information in intelligible form. The same rules apply also to request coming from abroad, i.e from individuals applying for visas to enter Malta.

The DPA can order the data controller to rectify, block or erase personal data. This service is extended by notifying the third party recipients of such an event, unless it involves a disproportionate effort. This information to third party recipient can be described as a best practice.

Complaints may be lodged by local citizens and by foreign individuals. The complainant may choose to remain anonymous or is entitled to ask the DPA not to disclose his identity to the data controller.

Complaints can be lodged both electronically and on hard-copy. A form is available on the website. A written routine issued by the Office further describes the procedure how to deal with a complaint and how to prepare the Decision. That document was made available to the expert. A Decision by the Commissioner is considered a sufficient basis to prove the breach against the Data Protection Act, thus allowing the data subject to sue the data controller for civil damages in the competent court.



## 3. SUPERVISORY ROLE (INSPECTIONS)

To enable investigations, the DPA has the right to enter any premises at any time and to access personal data being processed, obtain information on the processing of data and its security, enter and search any premises with the same powers as the executive police.

In the past inspections were carried out at casinos, the Government General Hospital, Credit referencing agencies, local councils, the Armed Forces of Malta and in commercial entities**.** Inspections of a technical nature were also carried out in police systems, Eurodac, and PISCES as well as in systems of commercial banks.

Experts were appreciative of the clear methodology that was used by the DPA, supported by written guidelines for Inspection procedures.

The procedure includes that a checklist is filled in after having conducted the inspection tasks and an inspection report is submitted to the Commissioner, thus ensuring that the follow up recommendations can easily be tracked. The DPA has the power to order certain measures like rectification or erasure. Notices to that extent may be appealed to the Court of Appeals within 15 days.

Any person aggrieved by a decision of the DPA may appeal to the Data Protection Appeals Tribunal.

Other inspection visits, mainly with respect to the security of systems, are planned in fall to the Europol and Interpol offices in Malta and to Consular offices (see below under "Visa issuance").



## 4. TECHNICAL SECURITY REQUIREMENT

### Protection of personal data

The National SIS system and also the SIRENE system will be part of the Police data network. There is a dedicated secure permanent connection from only authorised public services to the police by establishing different IPSec tunnels between public services and police, one per public service. The application level uses a centralized user management to grant and withdraw access to the application, based on a concept of the user profiles. Access profiles granted to police officers in relation to IT systems are reviewed whenever an individual officer is moved to another posting or service, is on extended leave or sick leave, or has resigned from the Malta Police Force. An administrative procedure is in place whereby these changes are notified to the Information Services Department by the Human Resources Section.

The quality control of alerts entered into the system is a task of the SIRENE office.

No technical copies are used outside the NSIS system. Training and testing of the system will be made by using dummy data.

There is no planning for a special law dealing with the NSIS and SIRENE measures. Experts recommend to check after the finalization of the SIS II legal instruments whether there is a need for submitting a special law.[1]

**Rules for logs**

NSIS system access log files will be kept by using network security management tools.
There will also use log files on the application level. All log files will be concentrated into a server where they can monitor if access is properly granted. The access to the log files is restricted to supervision purposes only.

Although the planned system is implementing well known technical solutions based on the experience of other members states, it should be noticed that the technical completion on time needs further efforts.



## 5. DATA PROTECTION IN RELATION TO VISA ISSUANCE

The Maltese consulates will not access SIS directly, because visa applications, along with the comments made by visa staff at the Embassy concerned, will be forwarded to the Visa Office within the Malta Police Immigration section of the Malta Police Force for checking against the SIS.

The awareness for Data protection rules in relation to visa issuance is strengthened by the training of personnel with respect to the implementation of the Data protection Act 2002, the appointment of a Data controller and a Data protection officer at the Ministry of Foreign affairs and by the visits, which the DPA plans to conduct to two consulates (possibly Moscow and Tripoli) this fall. In every embassy a Data protection co-ordinator has been designated.

[1] Malta will enact legislation providing for measures relating to the N-SIS and SIRENE measures.

The instruction that was circulated to the Embassies focuses on the purpose of collecting data for the issuance of visa, the secure storage of stickers and the retention of data.

Malta is invited to share with the Schengen Evaluation working party the results of this DPA visit to Moscow, in particular in order to establish a better understanding following the recent evaluation conducted by a Schengen team in that consulate.

## 6. INTERNATIONAL COOPERATION (COOPERATION WITH OTHER DPA)

Malta is an active contributor in the European cooperation and participates actively in the work of the Schengen Joint Supervisory Authority as well.

## 7. PUBLIC AWARENESS (INFORMATION POLICY)

The public is mainly informed about data protection in Malta by the website of the Commissioner. Experts were particularly appreciative of the efforts made by the DPA to organise seminars and conferences with a view to raise awareness on data protection to government entities, banks and insurance companies, schools, union's, professional bodies etc.

## AOB

- *List of documents which were made available to the inspection team:*
- *Inspection procedures. Guidelines*
- *Guidance for schools. Processing of visual images in schools.*
- *Guidelines for the promotion of good practice. Insurance business sector.*
- *Complaints procedures. Guidelines.*
- *Annual reports*

## 8. CONCLUSIONS AND RECOMMENDATIONS

***General conclusion***

The experts could consider that the Data protection rules in Malta comply with the requirements of the Schengen acquis, especially once a follow-up has been given to the recommendations mentioned below. The an impressive set of implementing measures, like guidelines, written procedures, training and awareness sessions, rank altogether as best practices among the Schengen partners. Malta is invited to confirm the follow-up to the recommendations in writing at a later stage, when reporting on the follow up of the current evaluations in the SCH-Eval group. [1]

*On the legislation*

1. Malta should formalise the application of the Council of Europe Recommendation at short notice.
2. It is recommended to check after the finalization of the SIS II legal instruments whether it is necessary to submit a special implementing law. The progress towards completion of the technical system may require additional efforts to be ready on-time.

*On the implementation*

*3.* . ---

*On the functioning*

4. Malta might consider publishing a manual explaining what the Schengen Acquis implies for the Maltese population, in particular in the field of Data protection.
5. Malta is invited to share with the Schengen Evaluation working party the results of this DPA visit to Moscow, in particular in order to establish a better understanding following the recent evaluation conducted by a Schengen team in that consulate.



[1] Reference is made here to the footnotes added by Malta to relevant parts of the report.