



Council of the
European Union

Brussels, 15 June 2018
(OR. en)

12748/06
DCL 1

SCH-EVAL 135
COMIX 747

DECLASSIFICATION

of document: ST12748/06 RESTREINT UE/EU RESTRICTED
dated: 15 September 2006
new status: Public

Subject: Schengen evaluation of the new Member States
- CYPRUS: 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.

RESTREINT UE



COUNCIL OF
THE EUROPEAN UNION

Brussels, 15 September 2006

12748/06

RESTREINT UE

SCH-EVAL 135
COMIX 747

REPORT

from : Data Protection Evaluation Committee
to: Schengen Evaluation Working Party

Subject : Schengen evaluation of the new Member States
- CYPRUS: Report on Data Protection

<u>1.</u>	<u>Legal base and organisational environment for data protection</u>	3
<u>2.</u>	<u>Data subjects and complaints handling</u>	7
<u>3.</u>	<u>Supervisory role (inspections)</u>	9
<u>4.</u>	<u>Technical security requirement</u>	9
<u>5.</u>	<u>Data protection in relation to visa issuance</u>	10
<u>6.</u>	<u>International cooperation (cooperation with other dpa)</u>	11
<u>7.</u>	<u>Public awareness (information policy)</u>	11
<u>8.</u>	<u>Conclusions and recommendations</u>	13

RESTREINT UE

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 Cyprus on 9-11 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 - Panayotis Nastou

I - Vanna Palumbo

LT – Vaida Linartaitė

SI - Jernej Lavrencic

SK - Peter Lieskovsky

CION - André Rizzo

CS - Wouter van de Rijt

PRELIMINARY REMARKS

The Cyprus 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 herself and her 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.

RESTREINT UE

Management summary

Data Protection in Cyprus with the view to applying correctly the Schengen acquis is by and large well prepared although experts found that in several cases, Cyprus should foresee in the introduction of detailed work routines; these routines should be developed by staff, the number of which seems currently insufficient to fully exercise an independent supervisory role¹. Additionally, important recommendations as to clarify the list of exempted authorities or as to the applicability of the Council of Europe Recommendation are submitted to the attention of the Cyprus authorities.

From a technical point of view, experts noted that Cyprus is planning to establish well known technical solutions in the implementation phase of the NSIS and SIRENE system based on the experience of other members states. The authorities are aware of possible problems and waiting for the SIS II legal instruments to finalise a special law.

1. LEGAL BASE AND ORGANISATIONAL ENVIRONMENT FOR DATA PROTECTION

Legal Framework

Data Protection rules in Cyprus are based on the following instruments:

The Constitution of the Republic of Cyprus, in particular the articles regarding Respect for private and family life and about the Secrecy of correspondence

The general Act on the Processing of Personal data (Protection of individuals) 138 (I) of 2001

It should be noted that neither the Police Act, N. 73 (I) 2004, nor the Administrative Act provide rules for Data Protection, which differ from the general rules. (*question to Cyprus: could you provide the team with a copy of the "Directions of the Data Protection Commissioner on police matters, as referred to in sheet 16 of the presentation by Elena on Tuesday morning ?*)

¹ Cyprus is of the opinion that, having in mind the size of the country, it is in a position to effectively exercise our supervisory role.

RESTREINT UE

Cyprus has implemented data protection rules laid down by the Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data of 28 January 1981; but it has not formally adopted the CoE Recommendation No. R (87) 15 regulating the use of personal data in the police sector, nor seems to have introduced an equivalent set of principles in its legislation.

Experts were told that this CoE Recommendation is already applied on an informal basis in Cyprus; Cyprus should however formalise this application at short notice, since this has actually become an obligation under art. 129 of Schengen, which entered into force in Cyprus on 1 My 2004, together with the other so-called "Category I" measures of the Schengen acquis¹.

Apart from this legal background, it is worth mentioning that the Data Protection Commissioner has the right to waive from certain crucial obligations under the Data Protection Act, among which the obligation to inform data subjects, certain data controllers if this data collection is performed for the purposes of defense, national needs or national security of the Republic or for the prevention, detection, investigation and prosecution of criminal offences, including processing of sensitive data. However, the list of these exceptions is not public, despite the fact that article 24 would allow the Commissioner to keep such a Register. Experts consider that citizens should have the right to know which bodies have been excluded from obligations under the DP Act.

These licenses to be excluded from DP obligations are granted by a decision of the Commissioner; there is no systematic follow up procedure, nor a review mechanism. The granting of this license is furthermore based on several concepts, including the concept of "national needs", which has apparently not yet been defined. This concept applies in particular in the case of the processing of personal data in the police sector. Experts consider that the current work going on in Cyprus to update legislation in the light of SIS II would offer an excellent opportunity to re-evaluate this procedure and in particular to give a public character to any decision or license exempting authorities from data protection obligations.

¹ Cyprus agrees with the recommendation that the provisions of Council of Europe Recommendation No. R(87)15 be introduced in the national legislation, be it the existing Police Law, a new Law regulating the use of personal data in the police sector, or any other legal instrument.

RESTREINT UE

It could for instance be decided to publish the list of decisions and licenses in the annual report and make that list available on the DPA's website ¹.

Experts were pleased to learn that the preparation to the implementation of Schengen in Cyprus is reviewed in a monthly meeting at the Ministry of Justice and Public Order to which the DPA is invited. Apart from that, there is an interdepartmental preparation of new legislation, to which the DPA is indirectly associated.

Organisation

The Office of the Commissioner for Personal Data Protection (later to be called the Data Protection Authority, DPA) has been established in May 2002. The Commissioner is appointed by the Council of Ministers, after consultation with the Parliamentary Committee for European matters. The required qualifications are the same as for a judge of the Supreme Court.

The Commissioner has no deputy, which obviously requires that proper work methods are found to ensure that there is no vacancy in the execution of the Office's competences.

The Commissioner has a staff of 6, out of which currently only one is a lawyer ², and one is an IT expert. These limited resources are due to a particularity of the Cyprus system of granting staff to public entities. The Commissioner cannot recruit her own staff, which could be better targeted and skilled according to certain needs, but the current staff is allocated from a central public authority. Experts are of the opinion that the limitation of the autonomy of the Commissioner to recruit its own staff, even if it should fit within a certain given budget, is a limitation to its capacity to handle and thus a limitation to its independence.

¹ Cyprus agrees with the recommendation that Commissioner's decisions waiving the obligation of the Police or other controllers to inform data subjects be published on our website and in the Annual Report (starting from the 1995 Annual Report which is in its final stage of preparation).

² At the moment of finalising this report, there is even no lawyer at all working for the DPA.

RESTREINT UE

The budget is an autonomous line in the State budget; it follows the general trend imposed on public administrations. Experts were told that the current level of the budget is sufficient to cover the operational expenses. However, no specific means have yet been foreseen to cover a public awareness campaign in connection with the implementation of the Schengen acquis.¹

A yearly report is made by the DPA and handed over to the Minister of Interior.² The DPA would consider it favourably if she was offered to present the report to the entire government and to the Parliament. Experts are of the opinion that the public presentation of the Annual Report is not only the occasion for the presentation of the work done by the Commissioner and the office but also gives the possibility to presents proposals for improving the functioning of the data protection system and make public misfunctions and problems arisen during the year.

It is though to be considered as an aspect of the independence of the DPA and not an “internal” duty of reporting about the activity done. Furthermore it is in the interest of the public to ensure a wide distribution of the report. The need to enhance the public awareness of the report is reinforced by the specific nature of the Cyprus legal system and the Data Protection law: many issues are not dealt in legislation and detailed procedures, thus leaving a certain unclarity for the citizens as to their rights. The introduction of written procedures would in general offer more security to the public.

The report is furthermore published on the website of the DPA.

¹ Cyprus has indicated that this might however change in 2007.

² The Law provides that the Annual Report is presented to the Minister of Interior. (The Law is going to be amended so that it will provide that the Annual report is presented to the Council of Ministers.)

In practice, however the Annual Report is officially presented to the President of the Republic and the President of the House of Representatives and on both occasions the press is notified about this.

The Annual Report is also sent to all Ministers of the Government, all Members of the House of Representatives, the members of the European Parliament, to all judges, advocates' associations, commercial banks, insurance companies, trade unions, the Chamber of Commerce etc.

RESTREINT UE

Due to the low number of complaints, or in general due to the small size of the country, the DPA deemed it until now unnecessary to adopt and publish written routines and procedures, other than the generally applicable standards for administrative acts. Common sense is applied on a case by case basis. Experts would however consider it useful if written practices were adopted and spread among interested bodies and possibly the public. Examples of such procedures to introduce are how to answer to a complaint, which methodology to use for an inspection, which rules to apply when cooperating with third countries, etc.

2. DATA SUBJECTS AND COMPLAINTS HANDLING

Right of access

The right of access of data subject is direct. This right should first be obtained at the data controller, before being entitled to launch a complaint. This means that in future, the request by the data subject shall be directly formulated at the Sirene Office. The data controller is supposed to answer to an applicant within 4 weeks. In case of a complaint at the DPA, there is no such a time limit.

The applicant has to pay a fee of 10 CY£ (approx. 15 €) per application. The fee is meant to support the costs of a file,. It seems that this sum is only applied in case of a complaint regarding the private sector and that it is often waived for the public sector. The fee is returned to the applicant in case his or her request is considered valid and granted.

Although one can understand that DPA's wish to avoid unnecessary and repeated requests by data subjects, experts are of the opinion that the system of requiring a fee is an undesired burden when wishing to make people better aware of their rights under the Data protection legislation. However, the EC Directive 95/46 only recommends that applications should without excessive expense.

RESTREINT UE

An applicant whose request was neither satisfied by the data controller nor by the DPA can appeal to the Supreme Court. This is necessary in Cyprus since there is no other judicial level between the Administrative or District jurisdiction and the Highest judicial authority. Experts wonder whether the costs linked to processing at the level of the Supreme Court are not dissuasive for the applicants. However, the Supreme Court is the only court which has first instance jurisdiction to hear and determine complaints relating to a decision by an executive or administrative authority. There is no other competent judicial or administrative authority dealing with such cases.

The answer given to a request for information is of the following nature: If information is held on somebody, the controller will write to the applicant that "no information is held, which the Police is by law bound to give". If no information is held, the applicant will be told that this is the case.

Experts recall their comment under Chapter 1 in which they wonder how the data subjects can use their rights if the list of public bodies which have been waived by the Commissioner under art 11 para 4 is not made public. Experts consider that whether this competence of waivering is given to the Commissioner or that in the new legislation the legislator should have this competence, the key issue is that there should be transparency of the list of authorities which are waived from Data protection obligations. (cf. also footnote 3)

The Commissioner mentioned a complaint about excessive information that was registered by the Police at the airport. After several unsuccessful efforts, the DPA succeeded in convincing the Police to modify the retention period and the content of these data. Experts consider that these successful mediations would gain of being made public on the website and thus raise the general interest of the public for data protection.

RESTREINT UE

3. SUPERVISORY ROLE (INSPECTIONS)

Experts were told that inspections took place at the Police, credit institutions, NSIS and the Central Bank.

However, since the DPA lacks the personnel and technical resources, these visits could not have the character of in-depth inspections.¹

The written reports tended to show that, for instance the inspection of the Police was merely a comparison between the original notification and the number of databases found in practice.

The experts recommend to develop a manual for conducting proper inspections and to allocate competent staff to these inspections.

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. All public services authorised to have access to NSIS system can access it through the Government Data Network where the police is also connected to. 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. As for the access to the NSIS by consulates, the consulates is connected securely to the Ministry of Foreign Affairs (MFA) by establishing an IPsec tunnel through the internet and then access to the NSIS system is granted through the secure channel from MFA to the Police where the NSIS system resides.

¹ Cyprus stated that the purpose of the inspection at the Police was to ascertain the accuracy of the contents of the Notifications submitted as regards the categories of data being processed, period of retention, recipients, processors etc.
As regards NSIS, as it is still not operational, the purpose of the audit was to be informed about the progress being made and the steps taken or to be taken for its proper functioning.

RESTREINT UE

The application level uses a centralised user management to grant and withdraw access to the application based on a concept of the user profiles. The access profiles, which have been granted, are reviewed when a police officer is moved to another service.

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.

It is planned to have a special law dealing with the NSIS and SIRENE. The finalisation of this law will be completed after the SIS II legal instruments have been adopted.

Rules for logs

NSIS system access log files will be kept by using network security management tools.

Log files will also be used 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.

Experts were told that the new system (see above) should be operational in all embassies by November 2006.

5. DATA PROTECTION IN RELATION TO VISA ISSUANCE

Access from embassies will be performed on-line and through a case by case system; this should thus not allow anyone to "shop" the NSIS article 96 database. Experts were informed about the efforts Cyprus is making to develop secure visa using a digital picture.

RESTREINT UE

From the point of view of Data protection, there are three issues that will continue to require attention: 1) the question of access to sensitive data by local staff, 2) the role of the Honorary Consuls ¹, 3) the capacity of the DPA to perform audits in the Consulates, since these do form an integral part of the national territory and thus the area of competence of the DPA.

Experts would welcome a reflection on the possibility to provide information in the Consulates as to the exercise of the right of access, rectification, etc.

6. INTERNATIONAL COOPERATION (COOPERATION WITH OTHER DPA)

Given the limited resources of the DPA, the experts were appreciative of the role and the involvement of the Cyprus representatives in the international bodies.

As far as the cooperation with other Data protection authorities is concerned, in particular when it comes to representing an applicant who asked for data that were introduced in another Member state, experts recommend that the DPA already now starts defining a working procedure in how it, in future, intends to deal with such cases.

7. PUBLIC AWARENESS (INFORMATION POLICY)

Experts were told that the level of public awareness of data protection in Cyprus is not very high.

The DPA should envisage which means could improve the situation. Several options were discussed, among which the possibility to launch a campaign once the Schengen acquis will enter into force, possibilities to add information on the website, possibly in languages which are useful to the numerous tourists who visit the island.

¹ Cyprus noted that in any case, Honorary Consuls will cease issuing visas, upon applying by Cyprus the Schengen acquis, in full.

RESTREINT UE

It has already been stated in this report that the public awareness is not triggered by the fact that the list of public bodies which are waived from several obligations under the DP act is not public.

AOB

Experts were given insight in a number of interesting documents, like the supervision report to the Police, a complaint about the Police at the border, bilateral agreements with both EU and non-EU states; Cyprus remains invited to send to the experts the Circular letter by the Chief of Police about data protection, to which it was referred in the presentation.

Experts welcomed the designation of one Contact point for Data protection within the Police. It is advised to give this contact point an increased visibility.

Experts appreciated too the external structure that has been created and which is in charge of supervising the police activity independently.

Experts were in general appreciative of the tight cooperation with police both on practical and on law-drafting level. Police also seems to put a lot of efforts on data protection.

Experts noted that no hierarchical authority is specifically tasked with the supervision of the DPA except through the auditing systems by the special controller of the state.

8. CONCLUSIONS AND RECOMMENDATIONS

General conclusion

The experts could consider that the Data protection rules in Cyprus will comply in future with the requirements of the Schengen acquis, once a satisfying follow-up has been given to the - quite numerous - recommendations mentioned below. Cyprus is invited to confirm this 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. Cyprus should guarantee the total independence of the DPA in particular concerning recruitment of personnel.
2. Cyprus should formalise the application of the Council of Europe Recommendation at short notice.

On the implementation

3. Cyprus should give a public character to any decision or license exempting authorities from data protection obligations.

¹ Cyprus is willing to follow the recommendations mentioned in this Report. As regards specifically the recommendations about introducing “detailed working routines” and “written procedures” these will be seriously taken into account as they promote transparency and awareness between citizens.
Cyprus stated however that the lack of these “routines” and “procedures” does not in any way affect or prejudice the proper and effective carrying out of our tasks and responsibilities, since these relate more to procedural questions.
As regards the staff of the Office, The DPA admits that there are problems due to the way the staff is recruited The draft Report however gives the impression that our Office is on the whole ineffective and cannot properly exercise any of its functions, a picture which we believe is not justified and does not represent the actual situation.
On the whole we observe that this draft Report is generally negative and is mainly focused on some, not always so substantial, in our opinion, issues and it does not contain any positive comment on the work done so far by the Office of the Commissioner.

RESTREINT UE

On the functioning

4. Written routines should be adopted and made available among interested bodies and possibly the public. Examples of such procedures to introduce are how to answer to a complaint, which methodology to use for an inspection, which rules to apply when cooperating with third countries, etc
5. Develop a manual for conducting proper inspections and allocate competent staff to these inspections.
6. Reflect on the possibility to provide information in the Consulates as to the exercise of the right of access, rectification, etc
7. Successful mediations would gain of being made public on the website and thus raise the general interest of the public for data protection.
8. The opportunity of the completion of the annual report should be seized to make a public presentation and to enhance the public awareness.
9. Define a working procedure on how to deal with requests for data that were introduced by another Member state
10. Launch a campaign once the Schengen acquis will enter into force in order to raise public awareness

Recommendation to the SCH-Eval group

11. Experts found useful the suggestion made by previous inspection teams to the Sch-Eval group and aiming at the possibility of a guideline being issued for the content of answers to be given to data subjects, both when no data are held and when data are held.