Council of the
European Union

Brussels, 31 May 2018
(OR. en)

8400/06
DCL 1

SCH-EVAL 64
COMIX 366

DECLASSIFICATION

of document:	ST8400 RESTREINT UE/EU RESTRICTED
dated:	13 April 2006
new status:	Public
Subject:	Schengen evaluation of the new Member States - HUNGARY: 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, 13 April 2006

8400/06

RESTREINT UE

SCHEVAL 64
COMIX 366

REPORT

from :	Schengen Evaluation Data Protection Committee
to :	Schengen evaluation Working Party
Subject :	Schengen evaluation of the new Member States - HUNGARY: 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 Hungary on 6/7 March 2006 according to the program mentioned in doc. 5014/06 SCH-EVAL 1 COMIX 4.

The following experts participated:

NO - Guro Slettemark (Leading Expert)
B - Willem Debeuckelaere
CY - Louisa Markidou
D - Ben Behmenburg
EE - Bert Blös
FIN - Reijo Aarnio
LV - Signe Plumina
NL - Niels Groenhart
P - Fernando Silva
S - Pehr Erik Jern
CION - Enikő Felföldi
CS - Wouter van de Rijt

PRELIMINARY REMARKS

The Hungarian 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 on Data Protection and Freedom of Information (hereinafter: DPA) 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 the previous 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

Experts are confident that Hungary is properly equipped both from a legal, a technical and a human point of view to exercise its competences in relation to the implementation of the Schengen acquis, provided that its competences will not be limited by the work going on in the Legal committee.

Since the Police has already initiated much work in relation to SIS-SIRENE, it is recommended that the DPA has a closer look at it and prepares its first inspection as the supervisory authority under art 114 of the Schengen Convention.

1. LEGAL BASE AND ORGANISATIONAL ENVIRONMENT FOR DATA PROTECTION

Legal Framework

Data Protection rules of Schengen relevance in Hungary are based on the following instruments:

- The Constitution of 1989, which provides the institution of the Parliamentary Commissioner for Citizens' Rights and the possibility for the Parliament to appoint specific Commissioners for the protection of certain Constitutional rights, among which the Parliamentary Commissioner for Data Protection, competent as well for Freedom of Information.
- Act LXIII of 1992 on the Protection of Personal Data and Public Access to Data of Public Interest (hereinafter: Data Protection Law), which has been amended in 2003, in order to define the rules for correction and deletion and in 2005 to define the rules of transfer to foreign authorities.
- Act LIX of 1993, which actually addresses the Parliamentary Commissioner of Civil Rights; however this Law serves as the basis for the Parliamentary Commissioner to report annually to Parliament on the outcome of his activities.
- The Police Act XXXIV of 1994 which contains several articles (or chapters) devoted to the implementation of the general data protection rules on the Police files

A draft Annex 5 to the HCNP`s Order, No. 11/2004. (VII.01.) of data protection and data security of Police contains the details on the physical security of the Police, including ILECC that hosts the SIRENE bureau operational from 1st August 2005 and the future SIS bureau (and also Europol, Interpol offices).

- Furthermore data protection rules laid down by Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data of 28 January 1981 promulgated by Act VI of 1998 and the Additional Protocol of 2001 regarding supervisory authorities and trans-border data flows promulgated by Act LIII of 2005 apply.
- Act IV of 1978 (the Criminal Code), amended several times since the, which regulates in its section 177 and further, 221 and 222 what is defined as Data protection related crimes.

No formal decision was made yet whether a specific SIS Act will be necessary, or whether it will be sufficient to amend several Acts. The DPA is of the view that it is not in the interest of Data protection in Hungary to specify that general data protection rules will be applicable to the specific case of SIS, since the absence of any specific measure would imply that the general rules continue to apply.

General data protection rules apply to all databases, both private and public (including national security agency files).

However the final status of data protection under the future SIS provisions is not precisely regulated yet, but since a legal committee has been set up within the Ministry of Interior, working on this issue- the adoption of the relevant EU legal acts on SIS II is awaited . Experts welcome the fact that the Parliamentary Commissioner for Data protection is full member of this committee. The relevant proposals to be submitted to the Parliament and the Government are expected to be ready before the end of 2006, which should allow Hungary to confirm to the Schengen evaluation group that the powers of the Parliamentary Commissioner for Data protection (later the DPA, for Data Protection Authority) will not be reduced in future with respect to SIS and SIRENE, in comparison with its current prerogatives.

The general rules foresee that the DPA is involved in a) the prior checking of databases, b) that is has the power to supervise and inspect the databases and the controllers and c) that it has the right to make incorrect data to be corrected or deleted.

Experts noted the difference of competence between the different functions of the DPA: whereas the correction or deletion of individual data can be met by a formal order issued by the DPA, to be implemented within 30 days, the DPA has only a right of opinion as far as the supervision of systems is concerned. This can lead to concern that the DPA would not be able to impose improvements in the management of data systems, even if these findings were the results of an inspection.

The Data Protection Commissioner and the Office (DPA)

Since 1995, the Hungarian Parliament elects by a two-third majority - and based on a proposal for a candidate by the President of the Republic - a Parliamentary Commissioner for Data protection for a 6 year-term, which can be renewed once.

The Commissioner is supported by a staff of about 44, including lawyers, 4 IT experts and administration professionals.

The Data Protection Commissioner is independent from the government, both functionally and financially. The budget procedure foresees that the Office of the Parliamentary Commissioners including the DPA have a special chapter within the budget and is separated from the budget from any Ministry. The budget has diminished in 2006 by 0,6 %, which is in line with the general financial policy of the Hungarian state. This will certainly put a constraint on several changes that have already been agreed, i.a. in relation to the Schengen implementation. Experts consider that it will be important to reflect in the budget for 2007 and the years thereafter the additional duties for Schengen, both in terms of new inspections and for the purpose of public awareness.

The DPA reports every year to the Parliament, a report that is made available on the Internet as well. The debate, both in the Commission and in plenary, is followed by a vote.

Apart from the competence for Data Protection, the Commissioner is competent as well for Freedom of Information.

2. DATA SUBJECTS AND COMPLAINTS HANDLING

The data subject may request information, the rectification or deletion of his personal data. The data subject has the right of objection and may institute court proceedings against the data controller in case of infringement of his rights.

The right of access by citizens to data in the SIS will in future be accessible through a request to the SIRENE bureau (right of access of a direct type), whereby the right of "appeal" for citizens will be exercised at the DPA.

Experts understand that at the current stage of preparation, these competences will indeed be devoted to the DPA; however they ask the Hungarian authorities to confirm that this will be the fact after necessary legislation or legislative amendments.

Access demands to the Data controller (the Sirene office) should receive an answer within 30 days, in an easy to understand way, according to art. 12 of the 1992 Act. A deadline that applies to all proceedings in public administration is not applicable to the DPA; however internal rules of the DPA state that possibly 30 days should be used for giving an opinion.

Experts were told that the Police Act gives the possibility not to give access to information and with the reason ; "there is no information we can give to you", only when query endangers the interest of a criminal investigation. Experts were puzzled by this possible confusing answer. It remains unclear for experts whether this reason would be also given if there were no data about the requesting person. Experts recommend that Hungary clarifies the situation with respect to this issue.

Experts also underline that they support the suggestion made by previous inspection teams to the Sch-Eval group aiming the possibility of a guideline being issued for answers to be given, both when no data are held and when data are held.

3. SUPERVISORY ROLE (INSPECTIONS)

1. Initiating the procedure

Ex officio inspection and inspection concerning a whole sector or a set of institutions can only take place on the initiative of the Data Protection Commissioner (DPA). Nevertheless a proposal for such inspection can be made by anybody but most of the inspections are based on the proposals of the DPA's colleagues. These inspections are based on:

- the number of complaints against an institution or data management
- preparatory work for legislation
- studying international trends, legislation, examples (e.g.. SMS marketing, CCTVs in the work place).

The inspections are carried out by the experts with the relevant experience in the given field or having the necessary expertise (e.g. computer science) designated by the DPA. Inspections involving dealings with classified information can only be carried out by the experts in possession of the security clearance issued by the Security Office.

2.Inspection methodology .

A letter signed by the DPA is sent to the head of the body to be inspected in the case of written requests. If the preliminary notice might endanger the success of the inspection, the data controller is visited without prior notice.

The data controller has to provide the answers for the written request within 30 days by the latest, in urgent cases within 8 or 15 days. In case of a missed deadline or the indication of non-cooperation the relevant supervisory authority or ministry is informed.

3. Closing of inspection

The inspection is closed with a statement summarising the experience written by the experts participating in the inspection and signed by the DPA.

4. Follow-up of inspections

The body investigated has to respond to the recommended measures by the latest within 30 days. In case the data controller does not comply with the recommendations of the DPA, he can order the suspension of data processing. In case of further non-compliance with the DPA's decision judicial procedure can be initiated. Further possible sanctions could be the publishing of the DPA's statement and/or requesting the responsible supervisory authority to take the necessary steps. The DPA reports to the Parliament about all his holistic inspections.

On the basis of the three cases given to the evaluation team by the DPA's Office on investigations done at different units of the national police and the NBI in different years the law enforcement authorities seemed to show willingness for co-operation with the DPA, keeping deadlines for providing the necessary information and respecting the recommendations of the DPA at the end of the investigation.

The DPA can not impose fines on the data controller. If the controller disagrees, the case must be handled by the court.

In 2005 the DPA performed 22 ex-officio investigations, while handling more than 1000 complaints in the field of data protection.

The DPA has not yet planned an inspection to the future SIS and SIRENE and expresses satisfaction with the current level of "cooperative preparation". Experts consider that this may not prove sufficient to comply with the formal role of the DPA to act as the supervisory authority over the Hungarian part of the SIS and recommend that there shall be at the most appropriate time an inspection on site, at the latest before implementation of Schengen. It can be argued whether this proactive inspection/verification to the SIRENE should take place already now that they are introducing Hungarian data, or shortly before the effective start of the system.

It remained unclear to the epxerts wthether there is an obligation for the SIRENE bureau to present the system to the DPA before it is made operational and is the Commissioner satisfied by the fact that he is only a member of two of the six consultation groups, the one looking into the legal questions.

The six consultation groups which are mentioned in the text refer to the internal project system of the Ministry of Interior which is set up from six professional projects coordinating and monitoring the preparation for the full Schengen membership as follows:

- Procurement and investment for construction (use of Schengen Facility)
- IT (use of Schengen Facility)
- Training (use of Schengen Facility)
- Institutional and organisational development
- Legal
- Schengen Evaluation

From the listed six groups the DPA is concerned in and involved in the IT project and the Schengen Evaluation project.
There is no yearly plan of inspections, the DPA is to a certain extent guided by the complaints it receives.

Within the police sector there are Data Protection Officers (DPO) in central, regional and local units. There are specific qualification requirements that have to be complied in order to be appointed as DPO, and they have important tasks and functions related to data protection and data security.

4. TECHNICAL SECURITY REQUIREMENT

Experts have been informed at the Hungarian National Police of the activities of its service to promote data security. Based on the relevant Hungarian legislation, the Police has implemented at every level, central, regional and local, the main principles of data protection, such as accountability, purpose limitation, data quality and security.

In general, it should be noted that these efforts by the Police were made at their own initiative, since the DPA was apparently not much involved in supervising the handling of Data protection rules by the Police in the case of SIS and SIRENE. Experts recommend that the DPA takes a closer interest in the coming months in the preparation of data security in relation to SIS and SIRENE at the National police.

Hungary's aim to use a smart card for protection the user password is very promising. Also the planned use for a PKI solution is very good from a security angle and will mean that many of the paragraphs in Art 118 can be fulfilled. If Hungary chooses not to be its own Certificate Authority if is of course vital that a trusted third part delivers the certificates.

The use of smartcards also opens for the usage of a strenghtened authentication which is recommendend by the experts.

The planned use of IPSec is also a very good approach, a s well as usage of thin clients. The experts were told that the final version of the system will also include a logging tool which gives the possibility to audit logs.

On one point there is need for clarification. The experts were puzzled about the fact that Hungary is planning to use WLAN. The expert team would like to have more information on this

Security rules are laid down on the physical protection of ILECC (e.g. entrances-exists, security), authorization of the staff (e.g. security, procedural). Four levels of security have been established, from basic to level III, with an increase of numbers and aggravation of applicable protection measures. Equipments have been put into place for providing security for case-handlings and administration (e.g. protection of computers and informatics network, cipher machines). Rules are laid down for qualification of documents, their archiving and also on the operation of CCTV.

Additional security rules are planned for co-operation and information exchange of international relevance in line with the international standards.

Experts are of the opinion that once SIS-test procedures will start, dummy data should be used; this point should be clarified during an inspection by the DPA.

5. DATA PROTECTION IN RELATION TO VISA ISSUANCE

The DPA has not yet been involved in the implementation of the Data protection rules within the Ministry of Foreign Affairs, which will host the Consular Information System; this system will be the interface between the Visa issuing department of the Ministry of Interior and the Consulates. Hungarian officials stated to the expert team that local staff in Consulates will have no authorization to access to SIS data. User authorization is regulated either by an expatriate IT expert of the diplomatic mission or consular post or by the Ministry of Foreign Affairs.

Experts recommend that the DPA be kept informed about this part of the work. In particular, it is recommended that the DPA verifies in how far proper access- and log rules have been set at all in the Consulates and how these procedures are maintained.

The DPA plans inspections in the consulates of Kyiv, Uzgorod and Belgrade later this year. Consulates form a part of the territory and the experts welcome this initiative by the DPA to visit consulates as a Best practice for the application of the Schengen acquis.

It remained however unclear whether the DPA intends to promote specific information about the rights of subjects for turned down visa applicants.

6. INTERNATIONAL COOPERATION (COOPERATION WITH OTHER DPA)

Cooperation with other Data protection authorities forms a part of the international activities of the DPA, which will materialise this year through the organisation of the Spring Conference of European Data Protection Authorities in 2006. In addition, the DPA takes part in the Working Party Art 29, and several other groups including JSA Schengen.
In cases where cooperation is needed with another Schengen member state in order to be able to reply to a request of access, the DPA plans to act on behalf of the applicant.

7. PUBLIC AWARENESS (INFORMATION POLICY)

Experts were appreciative of the efforts made by the DPA to promote information on Data protection through its website and in general about the pro-active attitude towards public awareness and raising attention in the media.

Experts welcomed the intention to look into the websites of other public authorities involved in Schengen, e.g; by suggesting to have links with the site of the DPA.

If the budget allows to do so, the experts feel that the implementation of the Schengen acquis in 2007 would offer an excellent opportunity to launch an information campaign to the citizens about their rights under the Schengen Information System.

Any other Business

Under the responsibility of the Ministry of Interior, a practical guide for Police officers, summarising the relevant parts of the Schengen Convention, the Handbook on Police cooperation, the Schengen catalogues has been publised inHungarian, awaiting new versions to be adopted by the EU.

8. CONCLUSIONS AND RECOMMENDATIONS

General conclusion

The experts are confident that the Data protection rules in Hungary will comply with the requirements of the Schengen acquis, once a satisfying follow-up has been given to the recommendations mentioned below. Hungary 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.

On the legislation

It is recommended do clarify by the end of 2006 when the work of the Legal committee will be completed that the powers of the Parliamentary Commissioner for Data will not be reduced in future with respect to SIS and SIRENE, in comparison with its current prerogatives.

On the implementation

Experts recommend that the DPA takes a closer interest in the coming months in the preparation of data security in relation to SIS and SIRENE at the National police, especially now that Hungary has already established a SIRENE-bureau which will issue alerts for future use in SIS.

It is recommended that there shall be at the most appropriate time an inspection on site, at the latest before implementation of Schengen.

Hungary is invited to provide additional information on its plan to use WLAN's.

The DPA should consider whether it is appropriate to use real data for testing purposes.

The DPA should be involved in the preparatory work at the MFA in relation with visa issuance.

Hungary is invited to develop plans for a campaign accompanying the implementation of the Schengen acquis in 2007.

On the functioning

Budgetary means should be adequate considering the fact that new tasks will befall on the DPA in the light of the Schengen implementation, i.a. a public awareness campaign, new inspections will be necessary, training of other public authorities.

The DPA should consider providing DPA specific information about the rights of subjects for turned down visa applicants.

Recommendation to the SCH-Eval group

Experts support 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.