Council of the
European Union

Brussels, 31 May 2018
(OR. en)

8401/06
DCL 1

SCH-EVAL 65
COMIX 367

DECLASSIFICATION

of document:	ST8401/06 RESTREINT UE/EU RESTRICTED
dated:	13 April 2006
new status:	Public
Subject:	Schengen evaluation of the new Member States - SLOVENIA: 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

8401/06

RESTREINT UE

SCHEVAL 65
COMIX 367

REPORT

from :	Schengen Evaluation Data Protection Committee
to :	Schengen evaluation Working Party
Subject :	Schengen evaluation of the new Member States - SLOVENIA: 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 Slovenia on 10/11 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 - Jacques Verraes
CS - Wouter van de Rijt

PRELIMINARY REMARKS

The Slovenian Data Protection Authority has 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 Information Commissioner 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 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.

Management summary

Experts are of the opinion that the DPA has the proper legal competences to act as an independent authority, but that it lacks the people and the budget to exercise its competences fully with respect to its Schengen obligations, including in advance of the implementation foreseen in 2007.

1. LEGAL BASE AND ORGANISATIONAL ENVIRONMENT FOR DATA PROTECTION

Legislation

The legal base for Data protection in Slovenia is built up of several instruments:

- Article 38 of the Constitution of the Republic of Slovenia, which states that," The protection of personal data shall be guaranteed. The use of personal data contrary to the purpose for which it was collected is prohibited.
  The collection, processing, designated use, supervision and protection of the confidentiality of personal data shall be provided by law.
  Everyone has the right of access to the collected personal data that relates to him and the right to judicial protection in the event of any abuse of such data.

- Aricle 39 of the Constitution, which states that " Freedom of expression of thought, freedom of speech and public appearance, of the press and other forms of public communication and expression shall be guaranteed. Everyone may freely collect, receive and disseminate information and opinions.
  Except in such cases as are provided by law, everyone has the right to obtain information of a public nature in which he has a well founded legal interest under law. "

- The Data Protection Act (Official Gazette of the Republic of Slovenia, No. 86/2004, as of 5 August 2004) which merged by January 2006 the Inspectorate for Personal Data Protection and the Commissioner for Access to Public Information into one independent state body, the Information Commissioner (IC)

- The Access to Public Information Act of 2003 (APIA), which is characterised by the fact that one doesn't need to motivate a legal interest in order to obtain information of a public nature.

- The Police Act (Official Gazette of the Republic of Slovenia no. 49/98) and the rules on keeping Police records (Official Gazette of the Republic of Slovenia, No. 122/2004 of 11 November 2004) which relates to the Personal Data Protection Act as a Lex specialis towards the Lex generalis. The Police Act specifies inter alia the rules on the manner of keeping police records and the rules on the protection of police data.

Experts are of the opinion that the legislation is both clear and explicit as far as the competences of the DPA are concerned and leave no doubt as to the hierarchy of legislation. However, the experts consider that it would be an asset if the DPA was closely associated to the work of the inter-departemental working groups, which prepare the implementation of the Schengen acquis.

Information Commissioner

(Duties, Powers, Accountability)

The Office was established in 2003 on the basis of the Access to Public Information Act. Its President is elected by the Parliament with a simple majority, on a proposal by the President of the Republic. The Commissioner for Access to Public Information (later to be called in this text the DPA, for Data Protection Authority) acts also as Information Commissioner
Due to this mixed competence, the Information Commissioner herself and the appointed four National Supervisors foreseen in The Data Protection Act art. 38 are entitled to see every document held by the Slovenian authorities, whatever its level of classification (DPA act art. 54).
The IC is appointed for a period of 5 years and may be re-appointed.

The budget of the DPA is currently of 327.000 euro. In, for instance, the supervisory department, there are currently only two inspectors, in charge of all sectors, both in the private and in the public field. Two more inspectors will be employed in the course of 2006. The procedure for adoption of the budget is according to the DPA Act art. 39 the following; Budgetary funds are determined by the National Assembly of the Republic of Slovenia on a proposal of the IC.

The Schengen evaluators are of the opinion that the current budget and staffing would not meet the requirements if the IC introduces a plan to Parliament showing that an additional number of supervisions will be necessary for the proper implementation of Schengen and a campaign of public awareness will be launched to accompany the putting into effect of Schengen. The DPA has apparently not yet been given the means to conduct inspections ex-officio, but only inspections based on a complaint that was lodged. The implementation of the Schengen acquis will on the contrary require that inspections be performed at the own initiatives of the IC.
The IC is also a minor offence authority, empowered to set the minimum fines whenever it finds infringements to the data protection rules. The product of these fines does not form a part of the financial means of the DPA. Those fines can be contested in Court.

2. DATA SUBJECT RIGHTS AND COMPLAINTS HANDLING

Data subjects can make requests for correction or deletion of files directly at the Police.
Within the Police, there is a Commission for personal data protection, whose duty it is to carry out the tasks related to the exercise of the rights of individuals for which the Police, acting as the data controller, are responsible.
Responding to a complaint when data has not been released or corrected, a data subject can launch an appeal at the DPA who has the power to order changes to be made. Apart from the appeal to the DPA, the data subject could also go to the Courts or submit the case to the Human Rights Ombudsman. The Ombudsman has however no powers in individual cases, but data protection is a special area of the Ombudsman according to the DPA act art. 59.
Complaints to the DPA are free of charge and can be made both in writing or even orally.
Experts consider the power to order to be an important tool to ensure the rights of data subjects.

Slovenian law demands a period of three months between two requests for access. Experts understands this time limit aims to prevent misuse. This rule applies only in uniform, same type cases in which the applicant states the same reasons for the access request. The DPA has however the right to rule on whether the request for access was refused on proper grounds.

Experts are however of the opinion that this time limit is bound to hamper the 'normal' exercise of data subjects rights, because it places the burden of possible misuse on the shoulders of the data subject which is not in compliance with the Schengen Convention and Convention 108 and R 87/15. If, in a certain case, data subjects rights are "used" or "misused" depends on the circumstances of the case. Therefore experts recommend that Slovenian law provides for the more open norm: 'at reasonable intervals' as does R87/15.

Slovenian law specifies for which police files exemptions to data subjects rights exist. Experts finds this very positive, because, as a consequence, for some police records it is without a doubt that access can not be refused. However, for the police records to which access of the data subject can be refused, Slovenian law (the Police Act) has bound the refusal solely and fully to a certain and entire formal moment in criminal proceedings.

This is bound to have as a consequence that data subjects will be longer deprived of there right of access than is indispensable for the justified interests named in the Schengen Convention (if indispensable for the performance of a lawful task or for the protection of the rights and freedoms of third parties). The possibility of granting access before this moment in time on a voluntarily basis is in this light not satisfactory, because it is only voluntarily. The same goes for refusal grounds in other specific acts such as the Aliens Act, of which it remains unclear if they also contain such exceptions.

Experts are of the opinion that it should be clarified whether other specific laws contains exceptions to the right of access and how these are formulated. Experts recommend that every such exception should enable the authorities and the DPA and courts, in the event of an appeal, to find a tailor made decision for cases at hand.

3. SUPERVISORY ROLE (INSPECTIONS)

The competencies of the inspectors and the right to enter onto premises, into buildings and to the liable person's devices are rules in art. 19 and 20 of the Inspection Act.

The Data Protection Act chapter 3 art. 53 gives the Supervisors competences to examine documentation relating to the processing of personal data, irrespective of their confidenitality or secrecy, and the transfer of personal data to third countries. The supervisors are entitled to examine the contents of filing systems, irrespective of their confidentiality or secrecy, and filing systems catalogues as well as examine documentation and acts regulating the security of personal data. Inspection measures are describes in the DPA act art 54, and gives the Supervisor the right to immidiately order:

- elimination of irregularities or deficencies he/she detects
- prohibition of processing personal data by persons in the public or private sector who have failed to ensure or implement measures and procedures to secure personal data
- prohibition of processing personal data and the anonymising, blocking, erasure or destruction of personal data
- to order prohibition of the transfer og personal data to third countries

For the violation of the provisisons of the Data Protection Act, the DPA have the power to impose fines relating to minor offences.

Experts were made available the outcome of a supervision performed vis-à-vis the General Police Administration with regard to video surveillance. The subpoena intimated the Police to file a written explanation on the use of video surveillance at certain premises and to correct possible irregularities. The deadlines set for explanation (15 days), and for correcting irregularities (30 days altogether), with a warning for a possible criminal and civil threat of liability of perjury and of a fine, convinced the experts that the DPA is well equipped to perform its supervisory function in an adequate manner.
However, with four inspectors employed by the end of June and three more legal advisers in the course of 2006, , the DPA does not yet seem to have the resources necessary to conduct inspections in both the private and the public sector, as it intends to do, the latter including an inspection to the SIS as well.

The DPA said that it did not intend to supervise the build-up of the current Schengen national databases, when it was asked by the experts if the DPA has scrutinised - or would do so in the near future - the measures adopted at the Ministry of Foreign Affairs on how to channel visa-related information (art. 96) between the SIS and the Consulates. The argument used by the DPA was that it wants to have free hands afterwards in its supervisory role, without being committed on the forehand. The experts are however of the opinion that it would be in conformity with art. 114 that the DPA verifies the adequacy and conformity of the data security and data protection before the moment the SIS will be launched in Slovenia.

4. TECHNICAL SECURITY REQUIREMENT

Rules on logs

The experts were informed that Slovenia will not work with a national technical copy of SIS but will access into the centralized system where all the data will be managed. The queries will be logged in a central log in Slovenia.

In this log the following data will be stored:

- internal (Police) users: data about each individual user;
- external users: data about organizations only.

For the external users logs with data about each individual user will be stored only within these organizations.

Networking

A combination of private and leased, encrypted lines are used. On the LAN´s the information circulates in clear text. Slovenia will in the near future use IPSec to encrypt all data traffic. According to the information that was given during the evaluation there is no physical separation between the internal network and the Internet connection. This can be considered as a risk and the experts recommend Slovenia to further look into solutions for strengthening the network security.

Autenthication

Slovenia trusts in user name and passwords for authentication. The experts recommend the use of strengthened autenthication method, e.g. within a PKI solution.

Slovenia has total a total number of 174 persons working in the framework of data security, informatics and telecommunications, of which 14 are working with information security. This is considered to be a good figure.

5. DATA PROTECTION IN RELATION TO VISA ISSUANCE

Experts were presented the scheme, which will be applied by the Ministry of Foreign Affairs to link its internal network with its consular representations, as well as the future VIS-SIS connectivity. It shows that, besides the tasks of the Police as the controller of the future SIS data, the Ministry of Foreign Affairs will have an important role to play with respect to art. 96 data, although it will not act as a controller with the right to enter or to remove data. There will be no direct access from consulates. Electronic means of communication will be provided for these purpose.
For the reasons explained under "Supervision", the DPA has not been involved until now with the preparations at the Ministry of Foreign Affairs; experts are however of the opinion that an interest in these plans forms a part of the responsibility of the DPA.

6. INTERNATIONAL COOPERATION (COOPERATION WITH OTHER DPA)

The DPA is an active contributor in the European fora on Data protection, although this participation was in the past limited by the small number of staff.
The IC is the authority who decides whether a third state (non-EU and non-EEA) satisfies the requirements of an adequate level of data protection, thus allowing to transfer personal data to these states.

7. PUBLIC AWARENESS (INFORMATION POLICY)

Under the title "Access to my privacy denied !", the DPA has published several brochures about the competencies of the information commissioner and the rules for access to public information in Slovenia. These brochures, coming along with the publicity for the new body, the fact that appeals can now be launched at an independent body and the launching of the SIS in Slovenia cast doubts as to whether the current staffing will be sufficient to properly reply within a decent time to the requests for information from the public.

8. CONCLUSIONS AND RECOMMENDATIONS

General conclusion

Having in mind that the Data protection legislation and in particular the structure of the Information Commissioner's office have only recently been established, the experts are confident that the Data protection rules in Slovenia will comply with the requirements of the Schengen acquis, once a satisfying follow-up has been given to the recommendations mentioned below. Slovenia 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

Experts recommend that the provisison on limitation period of three months between requests of access, should be formulated in a more flexible way e.g "..at reasonable intervals…"

Exceptions to the right of access should be examined and it should be clarified whether exceptions of the right of access will represent any obstacles in the Slovenian legislation concerning the implementation of the Schengen Convention.

On the implementation

Experts recommend that the DPA takes a closer interest in the coming months in the preparation of of the implementation of the Schengen acquis by the interdepartemental group set up to that end. The DPA should also be involved in the preparatory work at the MFA in relation with visa issuance and access rules in consulates.

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

Strengthen network security in the light of the absence of a physical separation between the internal network and the Internet connection.

Consider a strengthened authentication method

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

On the functioning

Budgetary means are insufficient to meet the requirements of the Schengen acquis as a active supervisory and inspection authority. It should be reconsidered in the light of the new tasks that will befall on the DPA in connection with the Schengen implementation, i.a. public awareness campaign, ex-officio inspections, 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.

_____