



Council of the
European Union

023281/EU XXVI. GP
Eingelangt am 28/05/18

Brussels, 28 May 2018
(OR. en)

6898/06
DCL 1

SCH-EVAL 32
COMIX 205

DECLASSIFICATION

of document: ST6898/06 RETREINT UE/EU RESTRICTED
dated: 3 March 2006
new status: Public

Subject: Schengen evaluation of the new Member States
- SLOVAKIA: 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, 3 March 2006

6898/06

RESTREINT UE

**SCHEVAL 32
COMIX 205**

REPORT

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

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

1.	Legal base and organisational environment for data protection.....	3
2.	Data subject rights and complaints handling.....	8
3.	Supervisory role.....	9
4.	Technical security requirement	10
5.	Data protection in relation to visa issuance	10
6.	International cooperation (cooperation with other dpa)	11
7.	Public awareness (information policy)	11
8.	Conclusions and recommendations	12

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 Slovakia on 2/3 February 2006 according to the program mentioned in SCHEVAL 1.

The following experts participated:

B - Georges Pijl (Leading Expert)

CZ - Jan Zapletal

D - Michael Nauth

HU - Ágnes Pajo

FIN - Reijo Aarnio

LV - Signe Plūmina

(Cion) Lukas Holub

(Council Secretariat) - Wouter van de Rijt

PRELIMINARY REMARKS

The Slovak 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 President of the Office for Personal Data Protection by attending and by contributing in person 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.

RESTREINT UE

Management summary

The experts have assessed that the foundation has been laid for the Slovak DPA, both from a legal, a technical and a human point of view, to exercise its duties in relation to the implementation of the Schengen acquis.

A separate legal Act for SIS II would clarify the role of the DPA and of all other actors, especially the relation between the internal and external control agencies.

The technical aspects of data security are well in place and available.

1. LEGAL BASE AND ORGANISATIONAL ENVIRONMENT FOR DATA PROTECTION

Legislation

The basic legislation for Data protection in Slovakia is built up of several instruments:

- The Constitution of the Republic of Slovakia of 1992, in particular articles 19 and 22, which guarantee the protection of privacy and family life and the protection against unwarranted collection, publication or other illicit use of personal data.
- The Act 428/2002 Coll. on Protection of Personal data, amended, which for the first time introduces a state supervision authority over the protection of personal data while processing personal data. (English version is available at:
http://www.dataprotection.gov.sk/buxusnew/generate_page.php?page_id=305)
- The Act 490/2001, which has amended the Act 171/1993 on Police Forces, extended the inspection powers of the state supervision authority also on personal data processed in police files and adding additional provisions for the processing of police data in police filing systems.
- The Act 10/1996 Coll. on control in the state administration, which establishes the obligation of internal control within public authorities.

RESTREINT UE

The legal base is further implemented within the Ministry of Interior by internal regulations of which the Decree of the Minister of the Interior N° 82/2005 on personal data protection in the information systems of the Police forces is relevant.

The links between the acts leave room for uncertainty as to whether the Office for Personal Data Protection (further mentioned under the acronym DPA for Data Protection Authority) has been made competent to supervise, inspect and possibly to sanction all state authorities.

Several sections of the Act 428/2002 shall not apply to the processing of personal data for safeguarding of the public interest, provided that the controller fulfils the obligations stipulated by a special Act determined for, among others, public policy and security and the detection and investigation of criminal offences. As a result several sections concerning the basic obligations of the controllers, information of the data subject and data subjects' rights do not apply. This is the case for the Police forces based on the Act 171/1993.

The experts are concerned about Section 69.4 of the mentioned Act stating that:

“(...) personal data registered by the police forces in compliance with the Act, shall be provided to (...) the Slovak Intelligence Service, to the Military Intelligence, to the Military Police(...)”.

The experts are furthermore concerned about the rivalry between the different legal Acts on the same subjects, i.e. processing of personal data and the rights of the data subjects.

The experts are even more concerned about the existence of a competitor for the DPA concerning the protection of personal data within the Ministry of the Interior, the Supervisory Bureau of the Minister of the Interior, which has been made the competent authority for all bodies and services within the competence of the Ministry of the Interior, including the police. This Bureau has been made competent for performing inspections, checking compliance with generally binding and internal regulations, supervisory duties, monitoring and disposing of complaints.

Although the experts understood that the Bureau should be considered as an internal controlling body, in compliance with Section 19 of the Act 428/2002, the legal basis of the Bureau and the relationship between the Bureau and the DPA need to be clarified. In any case, the Bureau does not comply with the requirements of Art. 114 of the Schengen Convention.

RESTREINT UE

During talks with the experts, it was stated that the DPA would exercise its full duties and competences, including the one to inspect, over the future SIS functions in Slovakia. This would indeed materialise the requirements of art. 114 of the Schengen Convention for an independent supervisory authority.

Consequently, experts could either recommend to rationalise the DP legislation as a whole or, at least, to clarify the rules applicable to the SIS in Slovakia in a separate legal instrument.

In particular, the experts are of the opinion that the future competence of the DPA as the authority to supervise and, if necessary, mandated to perform inspections to the SIS and the SIRENE Bureau should clearly be established.

That clarification should preferably be made in a separate legal instrument; if that happens not to be possible, experts suggest that at least a Memorandum of Understanding be formalised between the DPA and the Supervisory Bureau of the Minister of the Interior.

The Office for Personal Data Protection of the Slovak Republic (the DPA)

The DPA was established in 2002 and is a state administration authority with competence over the entire territory. The Office executes supervision of personal data protection independently and participates in the protection of the fundamental rights and freedoms of natural persons in the processing of personal data.

The DPA is led by the President of the Office, who is elected and recalled by the National Council (Parliament) upon proposal of the Government. He/she is assisted by a Vice-President.

Duties

The Office fulfils, among others, the following duties during execution of supervision of personal data protection:

- inspect continuously the state of protection of personal data, registration of filing systems and keeping of records concerning the filing systems;

RESTREINT UE

- recommend to controllers the measures for ensuring protection of personal data in the filing systems; for this purpose it shall issue recommendations for controllers within the scope of its power in the case of doubts whether the extent, contents and the manner of processing and use of the processed personal data are adequate to the purpose of their processing, are compatible with the respective purpose of the processing or whether they are not up-to-date as regards to the time and subject-matter in respect of this purpose, it shall issue a binding decision,
- in the case of suspicion that the obligations imposed by the Act were breached it may call the controller or the processor and request them for an explanation,
- provide inspection of the processing of personal data in the filing systems,
- impose sanctions in the case of determining that the obligations referred to in the Act were breached,
- submit a notification to the law enforcement agencies in the case of a suspicion that an offence was committed.

Powers

The chief inspector and other inspectors as well as the President of the Office and the Vice-President of the Office are entitled to:

- enter the lands, buildings or premises of the operations and facilities of the controller and of the processor,
- request from the controller, processor and their employees to provide them in a determined time limit with documents and other papers, opinions and information, data processed on storage media including technical data carriers, reports and source codes of programs, provided that they own them, and other records necessary for execution of the inspection, originals or copies and to enable them, in justified cases, to make copies also outside the premises of the inspected person,
- request from the inspected person to provide, in a reasonable time limit, complete and true oral and written information, opinions and explanations in respect of the inspected and related facts and determined deficiencies,
- require cooperation of the inspected person, etc.

RESTREINT UE

According to the President and the employees of the DPA, with the experts in session, the Chapters II and III of the Act 428/2002 (Activities of the Office and Rectification measures) are to be applied in full on the data systems of the Police Force and the future SIS.

Accountability

Although the DPA executes his supervision of personal data protection independently there are some doubts concerning the independent status of the Office. With the Act 428/2002 the lawmaker intended to give the Office an independent status in conformity with the international standards and requirements. The Constitutional Court of the Slovak Republic however, expressly confirmed that the granting of an independent status to a governmental body under a regulation with the force of a law, without such granting being based on and supported by the Constitution of the Slovak Republic, shall result in inconsistency of that law with the Constitution (PL. US 17/96. Ruling of the Constitutional Court of the Slovak Republic of February 24, 1998).

The DPA has only a limited budget autonomy, since the Office shall submit its proposal as a part of the chapter of the Governmental Office. The proposal is thus first subordinated to the general budgetary practice of the government, before being submitted to Parliament for consideration.

The budget amounted 25 million SKC in 2005 (665.465,00 Euro). The DPA's expectations on a budget increase for 2007 are estimated on the amount of 2,3 Million SKC.

The recruitment of staff reveals another issue of concern. The DPA is not fully independent in recruiting its personnel, since most of the future employees are to be recruited through the central Civil Service Office [Link: http://www.upss.sk/eng/zoznam_clankov.html?cast=42-4405]. For specific tasks, the DPA can call upon persons under contract but only temporarily.

The actual staff of the Office amounts to 25, mainly of academic level. There is a high turn-over in staff, approx. 30 % which poses risks to the amount and the quality of the work the DPA can deliver.

Experts underline the need to have an adequacy of means and tasks, 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.

RESTREINT UE

The DPA submits to the National Council of the Slovak Republic a report on the state of protection of personal data at least once in two years.

The experts are of the opinion that a fully independent status of the Office can only be ensured under the legal system of the Slovak Republic, through its establishment under the Slovak Constitution.

2. DATA SUBJECT RIGHTS AND COMPLAINTS HANDLING

The rules for access of citizens to personal data contained in data files is direct in Slovakia, according Section 20 of the Act 428/2002. The legal basis for the rules of access to police files however is the Act 171/1993, Section 69.

They include the right to request the Police Forces in writing for information on which personal data is being processed about a person. Police Forces are obliged to reply to the applicant without any fee in a period of 30 days from the admission of such a written application. Police Forces will on the grounds of a written application, without fee and without reasonable delay destroy or amend incorrect personal data concerning the person of the applicant. The Police Forces or the Ministry (of the Interior) shall, if they discover incorrect data, notify the applicant that these data have been destroyed; if they discover inaccurate data, they shall notify the applicant that the data have been amended and in other cases they shall notify the applicant, that his or her application has been examined.

The Slovak republic is invited to clarify in how far these rules limit the role of the Data protection authority with respect to Police files, in particular since paragraph 4 of the said section specifies that "For proceedings under sections 1 to 3 (*the provisions mentioned in the previous paragraph*), no general law on administrative procedure shall apply".

RESTREINT UE

Data subjects who do not agree with the answer they obtained to their request should appeal to the DPA. However, a complaint of a citizen might be dealt with either by the DPA or the Supervisory Bureau of the Minister of the Interior. Citizens have the choice, or follow both paths, leading thus to a case being investigated twice and in parallel. It has to be stressed however that an appeal to the Supervisory Bureau of the Minister of the Interior cannot be considered as an application of art.114 of the Schengen Convention on the independent statute of the authority to appeal to.

The Slovak authorities are invited to clarify these procedures and to make sure that for the implementation of the SIS there will be no misunderstanding possible.

3. SUPERVISORY ROLE

The chief inspector and other inspectors as well as the President of the Office and the Vice-President of the Office shall be entitled to:

- enter the lands, buildings or premises of the operations and facilities of the controller and of the processor,
- request from the controller, processor and their employees to provide them in a determined time limit with documents and other papers, opinions and information, data processed on storage media including technical data carriers, reports and source codes of programs, provided that they own them, and other records necessary for execution of the inspection, originals or copies and to enable them, in justified cases, to make copies also outside the premises of the inspected person,
- request from the inspected person to provide, in a reasonable time limit, complete and true oral and written information, opinions and explanations in respect of the inspected and related facts and determined deficiencies,
- require cooperation of the inspected person, etc.

The legal base and the prerequisites seem to be present to guarantee that the Office may be empowered to perform a proper supervision of the SIS.

RESTREINT UE

However, in practice, the Office has not yet given proof of their capacity to do so. Since 2002, no major government institution has been inspected. Furthermore, it remains to be confirmed in a dedicated SIS Act, or if that appears not to be possible, in a Memorandum of Understanding with the Supervisory Bureau, that the office can on its own initiative or following on a complaint, launch a full investigation into the SIS or the SIRENE Bureau, and do all inspection activities (with the full rights of access for people who are cleared, or with the assistance of the system administrator).

4. TECHNICAL SECURITY REQUIREMENT

Experts were extensively informed about the wide range of technical efforts made by the Ministry to ensure optimal information security and cryptography for the future SIS II and for the National Police Information Systems. Many preparations are underway, in particular at the Data Centre of Banska Bystrica, to establish the necessary technical and security standards. The level of security as it was sketched was considered to be impressive, with respect to the physical security, the management of the IT systems, the rules for access and the technical security measures.

5. DATA PROTECTION IN RELATION TO VISA ISSUANCE

Experts have extensively been briefed about the efforts made by the Ministry of Foreign Affairs and by the Central Visa Authority competent for Slovak visa consultations to do the necessary screenings and to run the IS Vision system in an appropriate manner. The internal cooperation with other departments is facilitated by the decision to establish an inter-departmental coordination group with the view to preparing the introduction of the VIS. The DPA is a participant in this group.

The DPA up to now, did not perform an inspection in a consular office abroad in order to check that no local staff is entitled to access the system, or that no officers be allowed to check the system other than for the purpose of handling a concrete visa application.

RESTREINT UE

6. INTERNATIONAL COOPERATION (COOPERATION WITH OTHER DPA)

Whereas Schengen evaluations usually address only the question of the cooperation with foreign DPA's, it should be underlined that the Slovak authority has in the first place to coordinate with the Supervisory Bureau of the Minister of the Interior. This Bureau will function as the internal supervisory body at the Ministry, with access to the SIS. Experts have suggested (see Chapter One) that the relation between the two bodies be formalised in a Memorandum of Understanding, whereby it should be understood that the Supervisory Bureau will act as the Office of Inspection according the Decree of the Minister of the Interior N° 82/2005 on personal data protection in the information systems of the Police forces and according article 19 of the Act 428/2002 Coll. on Protection of Personal data.

The Slovak DPA is an active participant in various international forms of cooperation among Data Protection authorities, thus proving an adequate preparation for future cooperation with other DPA of the Schengen countries.

7. PUBLIC AWARENESS (INFORMATION POLICY)

Experts welcomed the successful efforts to promote knowledge about Data Protection, i.a. by organising a seminar in February 2006. Much information is available on the website of the Authority.

The DPA should verify and assist the Ministry of Foreign Affairs and the Ministry of the Interior with the development of their websites, in particular with the rights of citizens in relation to Data protection.

RESTREINT UE

8. CONCLUSIONS AND RECOMMENDATIONS

General conclusion

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

2. It is recommended to clarify soon whether the implementation of SIS II will require specific legislation to supplement the general Data protection rules, harmonizing the overlap and rivalry between the legal bases and to clarify the competences and duties of all bodies involved in the future SIS. Especially the relation between article 69 section 4 of the Act n° 171/1991 Coll. on Police Forces and the future SIS regulations should be clarified.
3. Clarification is needed about the basic competences and duties for the DPA with respect to SIS II and the Slovak SIRENE office; that the office can on its own initiative or following on a complaint, launch a full investigation into the SIS or the SIRENE Bureau, and do all inspection activities (with the full rights of access for people who are cleared, or with the assistance of the system administrator).

On the implementation

4. The Slovak republic should guarantee the total independence of the DPA as an independent body defined in the Constitution and assure its operational independence, including a budgetary independence.

RESTREINT UE

5. It is recommended as well to clarify the relationship between the internal control (Supervisory Bureau of the Minister of the Interior) and the DPA. It should be made clear that the Supervisory Bureau of the Minister of the Interior cannot be the Supervisory body as meant in art. 114 of the Schengen Convention.
6. The Slovak Republic is invited to develop plans for a campaign accompanying the implementation of the Schengen acquis in 2007.

On the functioning

7. The Slovak republic is invited to clarify the competences of the Data Protection Authority with respect to Police files.
8. 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.
9. The DPA should consider paying a visit to a consulate and promote that no local staff is entitled to access the system, and that no officers be allowed to check the system other than for the purpose of handling a concrete Schengen visa application.
10. In the visa application procedure or together with the notification of refusal of the visa, a foreign citizen should be informed of his right of access, correction or deletion.
11. The DPA should verify and assist the Ministry of Foreign Affairs and the Ministry of the Interior with the development of their websites, in particular with the rights of citizens in relation to Data protection.