Council of the
European Union

**Brussels, 31 May 2018**
**(OR. en)**

**8399/1/06**
**REV 1 DCL 1**

**SCH-EVAL 63**
**COMIX 365**

**DECLASSIFICATION**

| | |
|---|---|
| of document: | ST 8399/06 REV 1 RESTREINT UE/EU RESTRICTED |
| dated: | 11 May 2006 |
| new status: | Public |
| Subject: | Schengen evaluation of the new Member States<br>- CZECH REPUBLIC: 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, 11 May 2006**

**8399/1/06 REV 1**

**RESTREINT UE**

**SCHEVAL 63**
**COMIX 365**



**REPORT**

| | |
|---|---|
| from : | Schengen Evaluation Data Protection Committee |
| to : | Schengen evaluation Working Party |
| Subject : | Schengen evaluation of the new Member States<br>- CZECH REPUBLIC: 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 the Czech Republic on 8/9 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 Czech 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 President of the Data Protection Authority by attending and by contributing in person 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 the Czech republic 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 the competences of the Data Protection Authority will not be limited by the amendments under preparation in the Police Act and other relevant Acts.
Before implementing the Schengen acquis, the DPA should look more closely at some technical security measures of the SIS and at the SIRENE office.



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

### Legislation

Data Protection rules in the Czech Republic are based on the following instruments:

- Art. 10 of the Charter of Fundamental Rights and Freedoms (i.e. Act No. 2/1993 Coll., promulgating the Charter of Fundamental Rights and Freedoms as part of the constitutional order of the Czech Republic)
- The Personal Data Protection Act (2000 by Act No. 101/2000 Coll.) is the basic legal regulation providing for personal data protection in the Czech Republic and implementing above-cited Art. 10 (3) of the Charter.
- The rules for personal data protection are also contained in many special regulations; in the area of public law, it is worth mentioning Act No. 283/1991 Coll., on the Police of the Czech Republic, Act No. 326/1999 Coll., on Residence of Aliens in the territory of the Czech Republic, or Act No. 13/1993 Coll., the Customs Act.

The legal picture is quite complex in the light of the fact that still more legal regulations apply, including the Penal Code, Certain information society services act, (No. 480/2004 Coll.) Act on register of population and birth numbers (No. 133/2000 Coll.) Electronic communications act, (No. 127/2005 Coll.) Act on identity cards (No. 328/1999 Coll.) Act on travel documents (No. 329/1999 Coll.).

The Czech Republic has furthermore implemented 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 Communication No. 115/2001 in the Collection of International Treaties and the Additional Protocol of 2001 regarding supervisory authorities and trans-border data flows.

It is not expected that the Czech Republic will prepare specific legislation to accompany the introduction of the SIS II. Nevertheless, several amendments to various legal acts are being prepared. From a point of view of data protection, no other Act than the Personal Data Protection Act No 101/2000 Coll. should be amended. No text proposals for the amendments to Act No 101/2000 Coll. have yet been forwarded to Parliament.

Experts would welcome that the amendment to the Police Act would specifically refer to the competences of the DPA over SIS.

Experts are of the opinion that the limitation of the scope of competences as now foreseen in art.2(2) of the Act No 101/2000 Coll. ("The Office shall be entrusted with the competence of a central administrative authority in the area of personal data protection in the scope provided by this Act") should be clarified in relation to SIS, either by amendment of this Chapter, or by amendment of the Police Act and other relevant acts, in order to comply with art 114 of the Schengen Convention. Also, a clarification should be given as far as art 3 (6) of the Personal Data Protection Act is concerned, in order to avoid that the competences of the DPA to supervise the SIS would be limited by the exemptions related to

(a) security of the Czech Republic,

(b) defence of the Czech Republic,

(c) public order and internal security,

(d) prevention, investigation, detection and prosecution of criminal offences,

(e) important economic interest of the Czech Republic or of the European Union,

(f) important financial interest of the Czech Republic or of the European Union, in particular the stability of financial market and currency, functioning of currency circulation and system of payments as well as budgetary and taxation measures, or

(g) exercise of control, supervision, surveillance and regulation related to exercise of public authority in the cases under (c), (d), (e) and (f), or

(h) activities related to disclosure of files of the former State Security.

**Inspector General for Data Protection**

The Office for Personal Data Protection (hereinafter "the DPA", for Data Protection Authority) is an independent supervisory authority, which was established in 2000 by Act No. 101/2000 Coll., on the Protection of Personal Data and on Amendment to Some Acts (the "Personal Data Protection Act").
The Office is headed by the President who is appointed by the President of the Czech Republic for a term of 5 years on the basis of nomination by the Senate of the Parliament of the Czech Republic. The President may be appointed repeatedly for another five-year term. The Personal Data Protection Act entrusts supervisory powers to 7 inspectors who are appointed for a term of 10 years by the President of the Czech Republic on the basis of nomination by the Senate.

Each year, the Office submits its annual report to the Senate and the Chamber of Deputies of the Parliament of the Czech Republic for consideration. The activities of the Office are financed from a separate chapter of the State budget, which is discussed and agreed by the Chamber of Deputies of the Parliament. The Office makes decisions on allocation of funds for its activities in its sole discretion.
The staff is composed of the President of the Office, 7 inspectors, a Supervisory activities section - 46 staff, the International department - 5 staff, a Press department - 4 staff, an Administrative and economic section - 20 staff.
The budget for 2005 amounts approx. € 3,2 million; 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.



## 2. DATA SUBJECT RIGHTS AND COMPLAINTS HANDLING

The data subject has the right to receive, to access, to request correction or deletion of his/her processed personal data. These rights should first be obtained at the data controller, before being entitled to launch a complaint. This means that in the future, a designated division of the Police Presidium (the System Control and Informatics Division - Personal Data Security and Control Group) will act as the Data Controller in accordance with the Police Act and collect all incoming requests from the data subjects concerning SIS II which will be passed to the Sirene Office.

A complaint may be lodged either at the DPA in its capacity of Data Supervisor, or at the Court, or with the Ombudsman. The Czech Ombudsman is however more concerned by addressing issues of mal-administration in general than by expressing opinions or orders about individual cases.
The Data protection authority is obliged to handle every complaint, according to the Administrative Act. The DPA would not set the step to the Court itself, but the Ombudsman could do so. A request for access is free of costs.
According to the Police Act, a data subject is only allowed to introduce a request for access once a year. This measure is motivated by the fear that some people would make an excessive use of their rights. Experts recommend that the provisions on limitation of periods between requests of access, should be formulated in a more flexible way e.g "..at reasonable intervals…".

Concerning the Personal Data Protection Act, there are no limitations on the frequency of requests.

Experts are also of the opinion that this time limit is bound to deprive data subjects of their fundamental right to access personal data relating to them. Experts suggest that Czech law be changed in this perspective and will limit the frequency of exercising the rights of data subjects to no more than 'reasonable intervals' as does R87/15 under Convention 108.

Experts were informed that Czech law does not require data subjects to state any relevant interest or purpose for which the data subjects exercises his/her rights.

Access can be denied if necessary to prevent that the accomplishment of police tasks in connection with criminal proceedings will be jeopardized, or the legitimate interests of a third person will be endangered. The reason for the decision on the refusal of the application must be given in writing. The reasons for refusal have to be mentioned.
However, if the police are not processing any personal data relating to the person, or the information about the reasoned decision would jeopardize the accomplishment of police tasks in connection with criminal proceedings, the requesting person shall be notified in writing that the police are processing no personal data relating to the requesting person. Experts were puzzled by this possible 'untrue' answer. It might give a data subject who is told that there is no data concerning him being stored, reason to believe that there are data to which access is denied.

On the one hand experts believe this can not be in conformity with the rule that refusal of access is only allowed if indispensable for a good performance of legal tasks. On the other hand this might give reason for a lot of appeals to the DPA in cases where there is no reason to deny the data subject the knowledge that there actually are no data stored.

Experts 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)

The Office is authorized to perform supervision over personal data processed by governmental agencies, local government, other public bodies and natural and legal persons and to perform control of automated processing or processing performed by other means
The supervisory role of the DPA is performed by 7 inspectors and an additional 12 employees.
Controls performed by the inspectors take place either on the basis of individual complaints or on the basis of the control plan (drawn up annually) as comprehensive controls of all duties in personal data protection.
In the field of police work, the Office has carried out four inspections during 2005:
Based on an anonymous complaint, the Office investigated if the police had taken any security measures to fulfil the obligations of article 13.1. of the Act 101 (also applicable to police forces in accordance with the provision of art. 3.6.).

The inspection demonstrated that the data controller (art. 13.1. of the Act 101) and some other persons (art. 14 of the Act 101) had violated the law.

The Office imposed specific measures in order to restore the correct application of the regulations; these measures are the object of a further appeal. The dispute is still pending.

Further to the investigation, concerning the application of article 11.1. of the Act 101 on temporary residence by citizens of the Slovak republic, the Office imposed two specific, improved measures and a fine on the police force concerned.

In an inspection about a.o. two different complaints (one regarding the police headquarters and another about a local police station) concerning biometric information – mainly fingerprints -, the Office inquired on a very large scale into the use and handling of this information. Audit records were requested, over 25.000 records were inspected (5% were checked on-site against the files and other documentation), and 27 offices in Prague and across the country were visited. Law breach (art. 5.1.d, e, f and art. 20.1. of the Act 101) was evidenced; consequently, a fine of CZK100,000 and five administrative improvement measures were imposed. The Office sent the Home Affairs Ministry a final note stating the problems in relation to the Act 101 regarding the existing legal framework for the processing by the police of fingerprints and sensitive data in general.

7 supervisions of the Police force and 1 investigation of the Ministry of Interior were carried out from 2001 tot 2005. Five supervisions are planned, 2 requests by the courts.



## 4. TECHNICAL SECURITY REQUIREMENT

Experts have been informed about the measures under preparation with respect to the workflow at the SIRENE office, the rules for access to the SIS, the authentication procedures, the Virtual Private Network at the Ministry of Interior and the plans for technical copies.

In general, experts were concerned that the current security measures deserve additional attention. The experts took note of the fact that the Sirene Bureau will use EVIN-SIRES as a workflow system. Such a tool is recommended in the Schengen Catalogue of Recommendations and Best Practices It seems that this best practice may be in contradiction with the Article 102 of the Schengen Convention.

The Czech Republic plans to use an additional technical copy at the airport of Prague. Another issue of concern relates to the authentication procedure, which uses passwords in plain text, which is not considered sufficient. Experts recommend the use of encrypted passwords. In the meantime, the Czech Republic informed the experts that - to protect the password, several tools of operating system are applied in the authentication procedure. To access the data, the Microsoft Explorer browser (light client) and the http protocol are used. Operating system Windows NT and/or upgraded versions are installed at central servers. "Integrated authentication" level has been set as "authentication method" in these versions of operating systems.

This arrangement ensures that the password is not transmitted as a plain text. Neither additional cipher protection nor https protocol is used.

One should look closely at the list of people having access to the logfiles, if the purpose of this access is not clearly defined.



## 5. DATA PROTECTION IN RELATION TO VISA ISSUANCE

Experts have been shown the future mechanism that will link the consulates abroad with Prague: the data transfer between diplomatic missions and the Ministry of Foreign Affairs will occur at given time sessions through secured digital lines (IP Sec protocol) and will be followed by a subsequent transfer from the Ministry of Foreign Affairs to the central body (Alien and Border Police Service Directorate) for security check.
In case of exceptional unavailability of the system, the visa procedure in relation to the Consulates will materialise through a single „read-only" SIS terminal at the Consular Department in Prague.
The DPA has been involved in a case study of the procedures for hiring staff in Consulates.
However, the DPA does not actually envisage a visit into a Consulate.
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.

It remained however unclear whether the DPA intends to engage in an effort to inform turned-down visa applicants over their rights.

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

Apart from its observer status in the JSA Schengen, JSA Customs, the DPA takes an active part in international cooperation, as well as having the role of vice-chairman of the JSB. Experts were told about interesting twinning efforts with Spain as well as support given to the development of a Data protrection function in Bosnia-Herzegovina.

## 7. PUBLIC AWARENESS (INFORMATION POLICY)

The DPA has already in the past developed activities with respect to public awareness. It intends to continue to inform the public in the future about Schengen with e.g. a web presentation and a flyer. This would supplement already existing efforts, like the Official Journal. 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. A table of actions to be taken in the process of preparation for Schengen mentions a public awareness campaign coordinated by the Ministry of Foreign Affairs.

The DPA announced its 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, so as to raise awareness for the rights of data subjects.

**AOB**

Experts were presented a list of Czech authorities with various rights related to SIS. In the current list of services or authorities entitled to access SIS, the DPA is supposed to be entitled to direct query to all alerts, by giving inspectors their own PC accounts. Having in mind that the right of access is direct, experts wonder if the DPA should be entitled to have such access. Right of access should for the DPA be limited to receive relevant documents when handling complaints, and right of access in situ – when carrying out general inspections/supervisions.

## 8. CONCLUSIONS AND RECOMMENDATIONS

***General conclusion***

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

It is recommended that the Amendments to the Police Act and other special acts, would specify the competences of the DPA over SIS and SIRENE and that no doubt remains as far as exceptions under Act 101 or special acts remain.

Experts recommended that the provision on limitation period between requests of access, should be formulated in a more flexible way e.g. "at reasonable intervals".

*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, since the workflow at the SIRENE office, the additional copy at the airport of Prague, the authentication procedure and the list of people having access to logfiles deserve additional attention.

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

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

The Czech Republic 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.

Reflect if the DPA indeed needs a direct access to SIS as an end user.

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.

_____