Council of the
European Union

Brussels, 28 June 2018
(OR. en)

14181/1/06
REV 1 DCL 1

SCH-EVAL 156
COMIX 859

DECLASSIFICATION

of document:	ST14181/1/06 REV 1 RESTREINT UE/EU RESTRICTED
dated:	7 November 2006
new status:	Public
Subject:	Schengen evaluation of the new Member States - LATVIA: 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, 7 November 2006

14181/1/06 REV 1

RESTREINT UE

SCH-EVAL 156 COMIX 859

REPORT

from :	Data Protection Evaluation Committee
to:	Schengen Evaluation Working Party
Subject :	Schengen evaluation of the new Member States - LATVIA: 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 Latvia on 19/20 September 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 - Jan Zapletal
I - Vanna Palumbo
NO - Guro Slettemark
CION - Carmen Guillen Sanz
CS - Wouter van de Rijt

PRELIMINARY REMARKS

The experts have valued the interest shown by the Inspector herself and her staff by attending and by contributing in person to the evaluation work. Important pieces of legislation, covering the different aspect of the Latvian legal system have been made available to the experts during their visit.

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.

Management summary

Latvia has developed or is in the process to do so the appropriate legislative framework for applying the Schengen acquis on Data Protection. However, serious doubts remain as to the independent status of the Authority, which is at this stage weak in the light of the requirements of art.114 of the Schengen Convention. Many efforts should be devoted too to develop the supervision functions of the Authority.

From a technical point of view, experts noted that Latvia is planning to establish well known technical solutions in the implementation phase of the NSIS and SIRENE system based on the experience of other Member states. The authorities are aware of possible problems. It is recommended to confirm after the finalisation of the SIS II legal instruments that the DPA is made fully competent as supervisory authority under the new special implementing law.

1. LEGAL BASE AND ORGANISATIONAL ENVIRONMENT FOR DATA PROTECTION

Data protection in Latvia is based on the following instruments:

- Article 96 of Constitution of Republic of Latvia, which states that " *every person has rights to his/her private life"*
- Law on adoption of Convention of Council of Europe for the Protection of Individuals with regard to Automatic Processing of Personal Data of 28 January 1981, No 108, which entered into force 12th April 2001
- Personal data protection law (PDPL) adopted of 23 March 2000, which entered into force 20 April 2000
- Regulation of liability for violation of personal data protection rules (amendments to the Latvian administrative penalty code of 1984) entered into force 15th April of 2003
- The Police Law of 1992, amended on 14 April 2005
- the Official Secrets law of 1997, amended on 26 February 2004
- Draft Law on the Schengen Information System

The Data Protection law is applicable in all sectors with an exception that is mentioned in article 4 of the PDPL " *protection of personal data declared to be official secret matters shall be regulated by the present Law with exceptions specified in the Law on Official Secrets".*
There is no specific Act implementing the 1987 Recommendation of the Committee of Ministers of the Council of Europe. Latvia should formalise this application at short notice, since this has actually become an obligation under art. 129 of Schengen, which entered into force in Latvia on 1 May 2004, together with the other so-called "Category I" measures of the Schengen acquis.
At the moment there is a draft law elaborated that contains amendments to the DP Law because the existing law is not close enough to the EU Directive 95/46. This draft contains in particular provisions that are aimed at sticking more to that Directive, in particular a better definition of controller, clarification on the scope of application, provision on the appointment of a “data protection officer” , notification system and transfer of data to third countries. The draft law also contains some rules on the Data State Inspectorate – section 24 - and introduces a new section – section 30- appointing the DSI as the sole supervision authority on the national section of the SIS and to ensure the respects for the data subjects’ rights.
Apart from that, Latvia is currently drafting specific SIS legislation.

The Office of the Data State Inspectorate

The Office of the Data State Inspectorate (later in this report to be called DPA, for Data Protection Authority) has been established in 2001. It supervises the Personal Data Protection Law, as from 2001, and the Freedom of Information Law, as from 2004.

The Office is headed by a Director who is appointed for a term of five year and (can be) dismissed by the Cabinet pursuant to the recommendation of the Minister of Justice. A Commission of the Ministry of Justice is set up to propose the nomination of candidates, after the vacancy was advertised.

The DPA was said to be acting independently in execution of functions provided in Law, although it is described as being under jurisdiction of the Ministry of Justice. Actually, the Constitution of the Republic of Latvia provides (in its article 58) that "The administrative institution of the State shall be under the authority of the Cabinet".

A Regulation of the Ministry of Justice (Regulation n. 243 adopted on the 29 of April 2003) defines the Data State Inspectorate as a state administrative institution subordinate to the Ministry (n. 24.5 of the list contained in part V) and, thus, on the basis of Article 1 of the said Regulation, the Ministry of Justice is described as the "superior institution for the State administrative institutions that are subordinate to the Ministry" . The fact that the DPA is embedded within the Ministry of Justice and the procedure of appointment and dismissal of its Director, although done for a fixed term of five years, leave thus serious doubts as to whether one can claim that the DPA is an independent body in the sense of art. 114 of the Schengen Implementing Convention.

In a similar way, the European commission has concluded that Latvia has not implemented the requirement under Article 28 of directive 95/46 in relation to the functional independence of the supervising authority of personal data . Consequently a working group has been officially set up with the task to prepare the legal acts necessary (Prime minister Order of January 2005) and has prepared a draft Amendment on the DP law.

The DPA is to be considered as being part of the Executive branch. The Director can be dismissed, like every other civil servant.

Experts are somewhat puzzled by this system, because it could affect the independence of the Director, in his/her relation with the offices to be evaluated. Even if the DPA is seen as a part of the executive branch, it would underline his independence of the rules for dismissal were made more similar to the ones applied for judges than for (top) civil servants

In any case, the implementation of the Schengen acquis would offer an excellent opportunity to better define purpose, tasks and power of the Data protection authority in order to grant it at least an effective and sounding "functional independence" in the sense required by the EU Directive on data protection. It is important to ensure the independence of the DPA by setting up specific procedures on dismissal, whereby the Director could have a higher level of protection against dismissal than civil servants.

Since the Schengen acquis sets requirements for the status of the independent supervisory authority, the Latvian system raises some concern, if there are no transparent and pre-defined criteria used for the assessment of the Director as a civil servant.

Experts recommend therefore to Latvia to adapt the legislation in conformity with the Schengen acquis by establishing a clearly defined independent status for the Director of the DPA. In the meantime, and until such legislation is in place, it is recommended that a Memorandum of Understanding be drafted between the Ministry of Justice and the DPA, which should describe the functional independence in the sense required by the EU Directive.

There has been a concept of Independent State Institutions accepted by the Cabinet of Ministers, according to it there would be new laws prepared which would apply to the Data State Inspectorate as well as to other state agencies (eg., the Financial and Capital Market Commission, Bank of Latvia, Public Utilities Commission). At first glance, and under reservation of a scrutiny of that legislation, this seems to be a way of enhancing the independence of the DPA.
Experts recommend also that the DPA be in a position to make proposals to legislation on its own, without being dependent of the hierarchy of the Ministry of Justice.

The staff has risen in recent years from 17 (in 2002) to 23 officials (in 2006). There is a high turn-over among the staff since salaries are not competitive with other services in Latvia. The DPA can rely only on a very limited number of IT specialists. Given the fact that the DPA is competent too for the Freedom of Information Act, one may assume that no more than 11 or 12 members of staff are on full-time basis available to perform the Data protection tasks.

The budget, however, has not risen accordingly. Figures show that the budget amounted € 324 573 in 2002, and after a peak of € 528 571 in 2003, it has fallen to 405 526 € in 2006. If one considers that the staff has risen from 17 to 23 and that Latvia has had an average inflation of 7 %, the budget seems insufficient to cope with the tasks the DPA is facing. The DPA lacks therefore the capacity to perform other necessary tasks, like unexpected inspections.

2. DATA SUBJECT RIGHTS AND COMPLAINTS HANDLING

The right of access

Individuals have a direct right *to request* information about the processing of their personal data.

1) the designation, or name and surname, and address of the system controller;
2) the purpose, scope and method of the personal data processing;
3) the date when the personal data concerning the data subject were last rectified, deleted or blocked;
4) the source from which the personal data were obtained unless the disclosure of such information is prohibited by law;
5) the processing methods utilised for the automated processing systems, concerning the application of which individual automated decisions are taken;
6) A data subject has the right, within a period of one month from the date of submission of the relevant request (not more frequently than two times a year), to receive the information specified in this Section in writing free of charge.

Experts were wondering whether this procedure is not hiding a limitation, since it would have been preferable to describe the subject's rights as the right to *access* information rather than the right to *request* information.

Also, art. 16 of the Personal Data Protection Law specifies that a data subject has the right to request that his or her personal data be supplemented or rectified, as well as that their processing be suspended or that the data be destroyed if the personal data are incomplete, outdated, false, unlawfully obtained or are no longer necessary for the purposes for which they were collected. If the data subject is able to substantiate that the personal data included in the personal data processing system are incomplete, outdated, false, unlawfully obtained or no longer necessary for the purposes for which they were collected, the system controller has an obligation to rectify this inaccuracy or violation without delay and notify third parties who have previously received the processed data of such.

Again, experts wonder whether it wouldn't have been preferable to lay the burden of proof on the Data controller, rather than on the Data subject. In any case, the procedure according to which the data subject has to find out himself - by turning to Data State Inspectorate or respective authority - in which database he or she is alerted is rather cumbersome.

Experts consider that all databases should be checked at once when a request is made to verify one database, the duty must be for the controller to check and find the data he has on the subject. Then if the data are not correct, the data subject has the right to have them changed, deleted etc. Latvia is invited to confirm that these rules are also applicable to processing of data by the Law enforcement authorities, and in particular for the Schengen system.

Experts suggest that data controllers would more actively help data subjects to use this right of access.

Decisions of the DPA may be appealed only to a court, which the experts value as an excellent procedure.

3. SUPERVISORY ROLE (INSPECTIONS)

To enable investigations, the DPA has the right to enter any premises without a prior written warning and to access personal data being processed, obtain information on the processing of data and its security, enter and search any premises with the same powers as the executive police. It has the right too to require that data be blocked, to bring an action in court for violations of the law, to impose administrative punishments, etc.

The legal prerequisites are thus not at stake. However, no effective in-depth supervision has taken place in recent years at key Ministries. It seems much more like the DPA is merely verifying the accuracy and the lawfulness of the notifications rather than performing inspections. There is an obvious reason for that: the staff is not equipped nor has it time to focus on this inspection task. DPA mainly carries out inspections based on individuals' complaints.

Instead of conducting in-depth technical inspections and supervisions, the DPA has in recent years been concentrating on its notification tasks, in particular by investing in a thorough manner in prior checkings. The following figures for 2005 are interesting in this context:

Notification of Systems:

- 625 systems in 2005
- 250 changes in Systems
- 1500 consultations about notification
-

Inspections:

- 168 inspections (including prior checking)
- 750 legal consultations

Another example of a task assigned to the DPA is to receive the Data protection Audit reports established by other State bodies (Ministry of Interior, Information Centre of Ministry of Interior, Border Guards, Office of Citizenship and Migration Affairs of Ministry of Interior).
It was not clear what the meaning is of this registration of reports, if the DPA has neither the time, nor the functional capacity to effectively inspect and supervise the data protection practices in these other state bodies.

Experts recommend that the DPA moves its priorities more into effective supervisions, rather than in the notification task. The latter one risks to turn the DPA into merely a registration office rather than being an active and independent guarantee of data protection of Latvia hampering eventually an effective supervision as required under art. 114 of the Schengen Convention. Experts doubt that the DPA would be able to inspect and supervise the SIS under the current situation, both with the limited number and (IT)-capacity of the staff and the heavy bureaucratic burden of notifications.
The level of fines, defined in the Latvia administrative violations code as amended in April 2003 with the introduction of specific provisions for unlawful processing of data (from 25 to 250 lats for physical persons and 100 to 1000 lats for legal persons, or from 100 to 1000 lats in relation to the different hypothesis considered), for failure to inform the data subject , lack of notification, failure to provide information to the DPA, failure to accredit to the DPA (25 to 250 lats) are considered insufficient to be dissuasive.

4. TECHNICAL SECURITY REQUIREMENT

The state of preparedness of the SIRENE-bureau, both the legal framework, the operational plans and the training of the staff has been presented.
Experts were slightly puzzled by the large number of authorities having access to the SIS. Even if the experts welcome that the DPA has access to all databases in Latvia, they do not consider it to be necessary to have for themselves, as DPA, access to the SIS, given the fact that their competence is to be able to supervise the system, rather than to use it.

Moreover, the large number of parties which have access could lead to using the SIS for more administrative purposes than for the ones it is designed [1].

Experts wondered also about the Internet connection that is foreseen, since systems with connection to internet may cause a risk for data security and thus to data protection and those vulnerable services like SIS II. Therefore it is essential, that the Latvian authorities update the data security level [2].

5. DATA PROTECTION IN RELATION TO VISA ISSUANCE

Representatives of the Ministry of Foreign Affairs sketched the security measures adopted between Riga (both the Ministry of Interior and the Ministry of Foreign Affairs) with the approx. 30 consular representations abroad, in order to ensure the best possible security of processing in relation to visa issuance.

Experts were pleased to note that the DPA intends to pay a visit to one or two consulates, where it can assess the compliance with data protection requirements in those countries the citizens of which require a visum to enter Latvia.

Experts were puzzled by the fact that apparently no procedure is foreseen to answer to a visa applicant whose application has been turned down. The answer given ("the person should just introduce a new request") is not satisfactory since it does not allow to highlight whether data are incorrect and should be modified or deleted.

[1] All institutions that will have access to SIS in Latvia have investigative powers. But in accordance with the national SIS draft law art.13 the officers can get an access to the SIS only if they act as persons and goods “controllers”. This means that access to SIS for the officers or other employees for administrative purposes is impossible.

[2] Despite the fact that the same infrastructure will be used (network, router) for data transmission the advanced methods for data protection and encryption (like VPN, DMZ, IDS, IPS) are used in personal data procession as well as other security arrangements (like user identification, passwords, etc.) which substantially reduces the risk of unauthorized access.

6. INTERNATIONAL COOPERATION (COOPERATION WITH OTHER DPA)

Latvia is an interested contributor in the European cooperation and participates in the work of the Schengen Joint Supervisory Authority as well. Furthermore, it is worth mentioning Latvia's participation in the Central and Eastern European Data Protection Authorities meetings, International Conferences for Freedom of Information Commissioners and Data Protection, TAIEX seminars, Baltic Region Conference on E-Commerce and Data Protection.

A project in the former Yugoslav Republic of Macedonia shows that Latvia has now become actively involved in the spreading of know-how on Data Protection.

7. PUBLIC AWARENESS (INFORMATION POLICY)

The DPA has performed in recent years the following activities in relation to the development of an Information strategy:

- 2001 – Informative work (seminars, meetings, brochure)
- 2002 – Explanatory and educative work
- 2003 – Survey on public opinion and determination of PR and Communication Strategy
- 2004 – 2005 - Implementation of PR and Communication Strategy (campaign on radio, TV and printed media); input from Phare project experts
- 2006 – new survey and improved PR strategy

The results of a survey are worth mentioning:

	2003	**2006**
Informed about the work of the DSI	23.3%	29.5%
Data Protection is not adequately ensured in Latvia	27%	52.9%
Inaccurate processing of personal data	10%	19.5%
More personal data requested than necessary for the specific purpose	6.4%	13.5%
Sensitive data in the hands of 3rd persons	7.9%	11.7%

Although this kind of results are always open to more than one interpretation, they show an excellent awareness of the DPA to address these issues.

AOB

List of additional documents which were made available to the inspection team:

The basic legislation as mentioned in Chapter One as well as

- Regulations n. 40 adopted on 30 Jan. 2001 Obligatory technical and organizational requirements for protection of personal data processing systems (issued according to art. 26 of the DP law)
- Regulation n. 217 adopted on 29 April 2003,Visa regulations
- Regulation n. 216 " " " , Procedure for utilisation, maintenance and updating of a list of aliens who are prohibited to enter the Republic of Latvia
- National security law adopted 16 May 2002 and lastly modified 1 December 2005
- State administration structure law adopted on 6 June 2002 (in force from January 1, 2003)
- Data state inspectorate annual report for the year 2005
- List of participants into the interdepartmental body coordinating the implementation of the Schengen acquis
- the draft SIS II legislation

8. CONCLUSIONS AND RECOMMENDATIONS

General conclusion

The experts are confident that the Data protection rules in Latvia will comply with the requirements of the Schengen acquis, once a satisfying follow-up has been given to the recommendations mentioned below, in particular with the sensitive question of the independence and with an enhanced focus on inspections.

Latvia is invited to confirm the follow-up to the recommendations in writing at a later stage, when reporting on the follow up of the current evaluations in the SCH-Eval group.

On the legislation

1. Even if some form of administrative embedding is necessary, the legislation should reflect a real independence of the DPA. Otherwise, this is contrary to the Schengen acquis and should be modified. In the meantime, and before the concept of Independent State Institutions is adopted, the independence in the sense required by the EU Directive may be formalised in a Memorandum of Understanding between the Ministry of Justice and the DPA.
2. Introduce the principles of the Council of Europe Recommendation (87) 15 in the legislation.

On the implementation

3. Experts suggest to reflect on the question whether the level of these fines is sufficient to be dissuasive.

On the functioning

4. The budget should be brought to a level which is sufficient to cope with the tasks the DPA is facing. The DPA lacks the capacity to perform other necessary tasks, like unexpected inspections.
5. Experts suggest that data controllers would more actively help data subjects to use their right of access.
6. Experts recommend that the DPA moves its priorities more into effective supervisions, rather than in the notification task .
7. It is recommended that the DPA confirms that the large number of authorities, which currently have access to the databases will not lead to using the SIS for administrative purposes.
8. Experts recommend to verify the security risk connected to the access of Internet.
9. Latvia should proactively inform turned down visa-applicants about their rights under the Data Protection legislation.