Council of the
European Union

Brussels, 21 June 2018
(OR. en)

14179/1/06
REV 1 DCL 1

SCH-EVAL 154
COMIX 857

DECLASSIFICATION

of document:	ST14179/1/06 REV 1 RESTREINT UE/EU RESTRICTED
dated:	7 November 2006
new status:	Public
Subject:	Schengen evaluation of the new Member States - ESTONIA: 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

14179/1/06
REV 1

RESTREINT UE

SCH-EVAL 154
COMIX 857

REPORT

from :	Data Protection Evaluation Committee
to:	Schengen Evaluation Working Party
Subject :	Schengen evaluation of the new Member States - ESTONIA: 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 Estonia on 21/22 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 Estonian Data Protection Inspectorate 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 Director himself 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 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

Estonia has a major problem to comply with the Schengen requirements because, contrary to art. 114, the Data Protection Authority is not competent to supervise the SIS, which falls within the remit of the State Official Secrets Act.

Furthermore, the inspection team is worried about the fact that Data Protection Authority is administratively subordinated to the Ministry of Interior and in this respect the Estonian system could raise some concern as far as the independence of the Authority is concerned.

Otherwise, the DPA would in many respects be well-prepared to implement all its duties according to the Schengen acquis.

From a technical point of view, experts noted that Estonia 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 Estonia is based on an extensive series of instruments:

- the Personal Data Protection Act, the second edition of which entered into force on October 2003, and was amended on 01.05.2004. The first edition of the Personal Data Protection Act entered into force on 16.07.1996;
- The Government of the Republic Act, which entered into force on 01.01.1996; the most recent amendment entered into force on 01.01.2006;
- The State Secrets Act, which entered into force 28.02.1999; the most recent amendment entered into force on 01.01.2006;
- The Data Protection Inspectorate Statute, the second edition of which entered into force on 07.06.2004. The first Estonian Data Protection Inspectorate Statute entered into force on 01.02.1999;
- The Databases Act, which entered into force on 12.03.1997 the most recent amendment entered into force on 28.04.2004;
- The Police Act, which entered into force on 08.10.1990; the most recent amendment entered into force on 01.06.2006;
- The Public Information Act entered into force on 01.01.2001; the most recent amendment entered into force on *01.01.2006.*
- + several decrees regulating the handling of DP within the Police. This seems on the one hand rather complicated a set of legal bases, it shows however a consciousness about Data protection within the Police.

Estonia ratified the Council of Europe 1981 Convention 108 for the Protection of Individuals with regard to Automatic Processing of Personal Data in 2000.

A working party which was established by the Ministry of Justice (2005) is working on the new version of the Personal Data Protection Act. Experts were told that the Data Inspectorate might lose executive powers of imposing financial sanctions to the government agencies and other state agencies [1].

A (future) SIS Act is currently under preparation; it will take into account the legal base, which will be established by the EU regulations and decision when adopted, because those acts are directly binding for MS and there is no need for a transposition into the national legal framework. It is indeed necessary to adapt the existing national provisions in order to fully comply with the new regulations on SIS II and remove any obstacle to the fulfilment of this goal (for example if there is a need to modify the penal code and the law on foreigners in order to consider the alerts entered in the SIS by the other States and the action to be taken –expulsion, discreet surveillance etc. – as if adopted by the national competent authorities).

There is no specific Act implementing the 1987 Recommendation of the Committee of Ministers of the Council of Europe. Estonia should formalise this application at short notice, since this has actually become an obligation under art. 129 of Schengen, which entered into force in Estonia on 1 May 2004, together with the other so-called "Category I" measures of the Schengen acquis.

The Office of the Data State Inspectorate

The Office of the Data Protection Inspectorate (later in this report to be called DPA, for Data Protection Authority) has been established in 1999

The office is headed by a Director who is appointed by the Government of the Republic on the proposal of the Minister of Internal Affairs for a term of five years. The head of the Inspectorate may not be appointed for office for more than two consecutive terms.

[1] There is no intention to remove any of the capacity to sanction from the DP. It is only as far as the financial penalties between different state agencies are concerned that Estonia envisages to abolish them. The responsibility within the public service is personal (disciplinary prodecures, misdemeanour or criminal case,) and will be taken care of by the Ministers in their own field of responsibility.

Administratively, the Director is entirely embedded in the structure of the Ministry and this seems to be contrary to the requirements of independence, as stated in the Recommendation (87) 15 of the Committee of Ministers of the Council of Europe and which states that every Member State is obliged to designate an independent authority outside of the police system that will be responsible for exercising supervision over the lawfulness of personal data processing.

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[1].

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

Experts recommend therefore to Estonia 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 Interior and the DPA, which should describe the functional independence in the sense required by the EU Directive.

[1] Estonia clarifies that the director of the DPA is appointed by the Government of the Republic, he or she can be dismissed only be the Government of the Republic, which is already higher degree than other civil servants.

There is an important limitation to the competences of the DPA, which is otherwise appointed as supervising authority for the vast majority of (private) databases in Estonia: the DPA is not entitled to perform supervisory duties into databases which are classified as State Secret. The State Secrets Act states in its art 4 (3) that information collected by the surveillance authorities on the basis of sections 115-120 of the Law of Criminal Procedure and the methods used for collecting the information, the tactics and the technical means in the scope that is necessary in order to use the information as evidence, is state secret classified as limited level (for example part of the personal data processing in police database KAIRI will be processed in national Schengen Information System). There seems to be a conflict of competence with art. 50 and 51 of the Databases Act, which on the contrary allow the DPA "the right to inspect at all times the compliance and the maintenance of state and local government databases with Acts and other legislation"

Experts cannot but conclude that the fact that the DPA will not be allowed to supervise the SIS is a clear breach of the requirements of art. 114 of the Schengen Convention.

The office has a staff of 23 officials, out of which 21,5 are occupied. All the officials are public servants, the Director is free to choose them. Considering that part of the staff is assigned to the other task of the Office, the Freedom of Information Act and given the current focus on notifications under the Data Protection duties, it is obvious that the size of the current staff does not allow the DPA to perform all the tasks it should be able to assume as an independent authority, i.a. as supervisor to the SIS.

The budget amounts 506.200 € in 2006, a figure which is foreseen to rise to 565.600 in 2007. This seems to be necessary if the DPA is supposed to fill the vacancies corresponding to the total foreseen number of staff, which amounts 31 and its scope of activity is widened.

2. DATA SUBJECT RIGHTS AND COMPLAINTS HANDLING

The right of access

At the request of a data subject, the chief processor and the authorised processor shall notify the data subject of the personal data relating to him or her, the purposes of processing of the personal data, the categories and sources of the personal data, third persons or categories thereof to whom transmission of the personal data is permitted and the name and address of the place of business of the chief processor.

A data subject has a right of recourse to the Data Protection Inspectorate or a court if the data subject finds that his or her rights are violated in the processing of personal data.

If the rights of a data subject are violated in the processing of personal data, the data subject has the right to claim compensation for the damage caused to the data subject. The DPA shall settle a complaint within thirty days from submission of the complaint, a term which may be extended to sixty days in order to additionally ascertain facts necessary for settling the complaint. The complainant shall be notified of extension of the term in writing.

Data subjects have to pay an amount of 3 Kroner (some € 0,20) per page of document that is issued to them, a procedure which the experts find unnecessary.

3. SUPERVISORY ROLE (INSPECTIONS)

Under the essential reservation made before that the Estonian DPA is not competent for SIS, the DPA is otherwise fully entitled to perform supervisory tasks on other databases, i.a. to apply administrative coercion pursuant to the procedure prescribed by the Acts, to initiate misdemeanour proceedings and if necessary impose a punishment, suspend the processing of personal data, demand the rectification of inaccurate personal data, prohibit the processing of personal data, demand the blocking or the termination of processing of personal data (including destruction or transfer to an archives).

This means that if the DPA was made competent to supervise the SIS, experts are confident that it would be able to perform these tasks in a correct manner, provided that the human resources would be brought up to the appropriate level. It would probably imply as well that the focus of the organisation be put more on inspection tasks rather than on the mere registration of new notifications or their update. The DPA does not even have to issue a pre-warning to inspect databases, which is considered excellent.

Experts were sceptical on the question whether the level of fines, be it when the offender is a physical or a legal person, is high enough to be dissuasive and suggest to the authorities to reflect on that.

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.

The SIS project is the largest IT project ever conducted within the Estonian Police.

Experts took note of the overview of access rights, clearly detailing which authority (Police, Security Police, order Guard, Customs and Tax Board, Citizenship and Migration Board, Vehicle Registration Centre) will have the right to provide data and/or the right to search data for the different categories of alerts.

The option to use Oracle was welcomed by the experts since this is considered to be an effective tool for maintenance and updating of the system, and thus granting a higher level of data quality. Since the Estonian network is not connected to open Internet, the system offers satisfying solutions to achieve better data security during data transfer.

The National Police Commissioner (Police Board) has drawn up an extensive set of orders regulating IT and data protection. Some of the orders function as a basis for inspections performed by the DPA.

During talks with the experts, the level of awareness of the rules governing the transfer of data to third countries appeared to be insufficient. Estonia should inform all involved bodies of the obligations under the articles 28 and 14 of the Personal Data Protection Act, including the role therein of the DPA.

5. DATA PROTECTION IN RELATION TO VISA ISSUANCE

Representatives of the Ministry of Foreign Affairs sketched the security measures adopted between Tallinn (both the Ministry of Interior, the Ministry of Foreign Affairs, the Citizens and Migration Board and the Board of Border Guard) with the 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 has asked to the Ministry of Foreign Affairs to arrange 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 Estonia. This initiative deserves to be applauded, although experts consider too that it should be the right of the DPA to do such a visit, and not something for which authorisation should be seeked.

Experts were puzzled by the fact that apparently no procedure is foreseen to warn an applicant of his/her rights under the Data protection legislation, including the right to ask for correction or deletion of data that appear to be wrong, when his 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.

6. INTERNATIONAL COOPERATION (COOPERATION WITH OTHER DPA)

Estonia 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 Estonia's participation in the Central and Eastern European Data Protection Authorities meetings, International Conferences for Freedom of Information Commissioners and Data Protection, Commissioners TAIEX seminars, Baltic Region Conference on E-Commerce and Data Protection.

7. PUBLIC AWARENESS (INFORMATION POLICY)

The DPA is developing efforts to raise awareness in Estonia for data protection through its website (http://www.dp.gov.ee) which contains all necessary information, be it that the English version could be somewhat further developed. Typically, it is the Ministry of Interior, and not the DPA itself, which is mentioned as the publisher of the site[1].

Furthermore, the staff of the DPA tries to raise awareness by participating in training sessions and conferences and by publishing articles.

AOB

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

- The legal acts referred to in Chapter one
- and an overview of Cross-border police cooperation with Finland

8. CONCLUSIONS AND RECOMMENDATIONS

General conclusion

The experts would have been confident that the Data protection rules in Estonia 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 functional independence if a crucial element was not missing, which is the competence for the DPA to effectively supervise the N-SIS. In that respect, Estonia is in breach of article 114 of the Schengen Convention.

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

[1] This error appears in the English version of the site and will be corrected to highlight the role of the DPA as editor of the website.

On the legislation

1. Estonia should designate the Data Protection Authority as supervisor over the SIS and allow the DPA to effectively perform all supervisory functions.
2. 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, until the legislation is modified, the independence in the sense required by the EU Directive may be formalised in a Memorandum of Understanding between the Ministry of Interior and the DPA.
3. Introduce the principles of the Council of Europe Recommendation (87) 15 in the legislation.

On the implementation

4. Raise awareness among the relevant authorities for the competence of the DPA when transferring data to third countries
5. Experts suggest to reflect on the question whether the level of the fines is sufficient to be dissuasive.

On the functioning

6. Estonian authorities should ensure that there will be staff available for the further tasks of the DPA, i.a supervision of SIS.
7. Estonia should proactively inform turned down visa-applicants about their rights under the Data protection legislation