Council of the
European Union

Brussels, 28 May 2018
(OR. en)

6897/06
DCL 1

SCH-EVAL 31
COMIX 204

DECLASSIFICATION

of document:	ST6897/06 RESTREINT UE/EU RESTRICTED
dated:	3 March 2006
new status:	Public
Subject:	Schengen evaluation of the new Member States - POLAND: 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, 3 March 2006

6897/06

RESTREINT UE

SCHEVAL 31
COMIX 204

REPORT

from :	the Schengen Evaluation Data Protection Committee
to :	Schengen evaluation Working Party
Subject :	Schengen evaluation of the new Member States - POLAND: 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 Poland on 30/31 January 2006 according to the program mentioned in doc. 5014/06 SCH-EVAL 1 COMIX 4.

The following experts participated:

B - Georges Pijl (Leading Expert)
D - Michael Nauth
HU - Ágnes Pajo
FIN - Reijo Aarnio
SI - Dejan Žorž Zaviršek
(Cion) Piotr Rydzkowski
(Council Secretariat) - Wouter van de Rijt

PRELIMINARY REMARKS

The Polish 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 Inspector General 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

The experts have assessed that the Polish DPA is properly equipped, both from a legal as from a technical and human point of view, to exercise its duties in relation to the implementation of the Schengen acquis.

Experts regretted however that much of the regulatory work and of the security measures relating to the introduction of SIS (II) and the SIRENE office are neither in place nor firmly decided at this stage.

It is recommended that the Bureau of the Plenipotentiary of the Government for Preparation of the Authorities of Public Administration to the Co-operation with the Schengen Information System and Visa Information System, should closely work together with all interested and relevant partners (DPA, Police, Border Guard, Consular services + other authorities) to share information and to monitor closely the work in progress.

There is a need for closer co-operation between the Bureau of the Plenipotentiary and the Polish Data Protection Authority.

1. LEGAL BASE AND ORGANISATIONAL ENVIRONMENT FOR DATA PROTECTION

Legislation

The legal grounds for granting the protection to personal data in Poland include two provisions of the Constitution of the Republic of Poland of 2 April 1997 which provide for the protection of private and family life, honour and good reputation and making decisions about one's personal life (Art. 47 of the Constitution) and stipulate that no one may be obliged, except on the basis of statute, to disclose information concerning himself/herself (Art. 51 paragraph 1 of the Constitution).

The Constitution indicates also obligations and limitations for public authorities.

The legal act regulating the issues related to personal data processing in Poland is the Act of 29 August 1997 on Personal Data Protection (Journal of Laws of 2002 No. 101, item 926) which entered into force on 30 April 1998.

Moreover, on 24 May 2002 Poland ratified the Convention of the Council of Europe No. 108 of 28 January 1981 for the Protection of Individuals with regard to Automatic Processing of Personal Data, and then introduced its text into the national legal system by announcing it in the Journal of Laws of 2003 No. 3, item 25. In July 2005 Poland ratified the additional protocol to the mentioned Convention (published in the Journal of Laws of 2006 No. 3, item 15).

The Act on the Protection of Personal Data of 29 August 1997, with later amendments, (English version available at: http://www.giodo.gov.pl/data/filemanager_en/61.pdf)) is of paramount importance for the issues related to personal data protection in Poland. It regulates the activity and competencies of the personal data protection authority, the principles of personal data protection, the data subjects' rights, the issues regarding safeguarding personal data, registration of personal data files, transfer of personal data to third countries and criminal liability.

Experts were concerned by the obvious uncertainty as to whether the implementation of the SIS II will require specific legislation to supplement the general Data protection rules. According to the answers on the Questionnaire 9820/1/05/REV 1 ADD 1, a future Act on SIS specifying data protection procedures in connection with use of the SIS and the development of the SIRENE Bureau is the subject of consultations at the Ministry of Interior. But different views were expressed by the interlocutors at the DPA and at the Police, although it is rather urgent to deliberate on this.

The Evaluation Committee has been informed by the Inspector General that the Bureau of the Plenipotentiary of the Government for Preparation of the Authorities of Public Administration to the Co-operation with the Schengen Information System and Visa Information System, while working on the principles of a proposal of the act governing the operation of so called Polish Component of the SIS II, did not forward to the Polish DPA the draft with the request for consultation, depriving the DPA of the knowledge on the principles of the Polish part of the Schengen Information System. This also precluded the Inspector General from exercising the duties referred to in Article 12 point 4 of the Act on the Protection of Personal Data. A request to clarify this situation has been addressed to the Minister of Internal Affairs and Administration.

Experts are of the opinion that the DPA should in any case ensure that specific legislation would in no way limit the scope of its current competences. This is in particular the case in relation to the appeals procedure, (see also chapter 2) which should remain within the remit of the independent authority in order to comply with the Convention 108 of the Council of Europe. Poland shall inform the Schengen Evaluation WP at the moment it will report on the follow up to this report that the competence for appeals has not been transferred to the Ministry of the Interior (which would otherwise be in the position to "control the controllers").

It is necessary to answer the question if the controller of data managed in the future SIS will or will not be considered as a controller of data constituting a state secret because of state security, protection of life and limb of people, property or public safety and order. If this should be the case, the powers of inspection of the Inspector General will be rather limited.

According the explanations given by the Inspector General, the exception clauses of art 43.2 of the Act (which seems to apply to internal and external State security services as well as military intelligence services), and which would minimise the role of the DPA considerably, do not apply in case of data files containing data that were collected as a result of inquiry procedures held by officers of the bodies authorised to conduct such inquiries processed by the Police. In this concept the information managed by the SIRENE bureau through the SIS II would fall under the full competence of the DPA.

Inspector General for Data Protection

The law foresees that the supervisory authority for the protection of personal data shall be the Inspector General for Personal Data Protection. The independence and the authority of the Inspector General are guaranteed by several strict requirements about appointment and dismissal, immunity and financial conduct of the authority.

Duties

Pursuant to Art. 12 of the Act on Personal Data Protection the duties entrusted to the Inspector General comprise:

1) supervision over ensuring the compliance of data processing with the provisions on the protection of personal data,
2) issuing administrative decisions and considering complaints with respect to the enforcement of the provisions on the protection of personal data,
3) keeping the register of data filing systems and providing information on the registered data files,
4) issuing opinions on bills and regulations with respect to the protection of personal data,
5) initiating and undertaking activities to improve the protection of personal data and
6) participating in the work of international organisations and institutions involved in personal data protection.

Powers

In order to carry out the duties referred to in Art. 12.1 and 2, the Inspector General and employees of the Bureau are authorised to:

1) enter any premises where data filing systems are kept and/or processed and to perform all necessary inspections,
2) demand written or oral explanations,
3) consult any documents and data directly related to the inspection,
4) perform inspections of any devices, data carriers and computer systems used for data processing,
5) commission expertise and opinions to be prepared.

The inspector performing the inspection as mentioned in article 43.1 and 1a of the Act (data on state security and public order; data collected as a result of inquiries held by officers authorized to conduct such inquiries) is only authorized to consult data files in the presence of a duly authorized representative of the unit under inspection. In the case of Art 43.1 the powers of the Inspector General will be limited in so far as he/she will not enjoy the power to perform direct inspections; handling complaints, demand to demonstrate documents and data and demand to render devices, information media and systems used to process the data available for inspection.(See also the Supervisory role).

Accountability

The Inspector General is subject only to the Act and once a year he/she shall submit to the Diet (The lower house of the Polish Parliament) a report on his/her activities. Accountability about the financial conduct is guaranteed by a yearly control by the Supreme Chamber of Control.

The Inspector General's independence is guaranteed by the fact that the authority has a separate budget, accepted by the Parliament, which constitutes a part of the State's budget (next to the government's budget). The budget of the Polish personal data protection authority is not a part of the budget of other institutions (e.g. the Ministry of Justice or the Ministry of Internal Affairs and Administration).

It was noted that the budget for 2006 was slightly below the 2005 level. 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.

Other new tasks will also befall in the near future on the DPA, such as the role of trusted third party in relation to electronic signatures.

The Inspector General for Personal Data Protection performs its duties assisted by the Bureau of the Inspector General for Personal Data Protection The total number of employees of the Bureau is 116 persons, including 68 lawyers (i.a. in the Legal Department, Complaints Department, Inspection Department), 13 IT specialists and a press team.

2. DATA SUBJECT RIGHTS AND COMPLAINTS HANDLING

Data subjects have a direct right of access in Poland.

Art. 24 and 25 of the Act specify the information which shall be provided to the data subject by the controller after collecting his/her data. These do form an obligation for the controller. It includes information on the purpose of data collection, about the data recipients or categories of recipients; right of access and rectification of personal data by the data subject;

Articles 32 and 33 of the Act detail inter alia the rights of access and rectification of personal data by the data subject.

The controller may refuse the right to access to the filing system if it results in the disclosure of the information constituting a state secret or poses a threat to national defence or security of the state, human life and health, or security and public order; poses a threat to fundamental economic or financial interests of the state or results in a substantial breach of personal interests of the data subjects or other persons.

Experts were told that "*The Inspector General considered a complaint on the actions of the Chief Commandant of the Police who referred to the above mentioned exclusion and refused to provide the complainant with the requested information concerning him. In this case the Inspector General acknowledged by means of administrative decision that the realization of the right to control the processing of personal data by making data available in the scope requested by the complainant would result in a breach of provisions of the Act on the Protection of Personal Data by causing a threat to national defence or security of a state and public order (Article 30 point 2 of the Act)".*

The refusal should be subject to control by the Inspector General by examining the legality of the procedure of introducing the objection to the system. According to the ruling of the Supreme Administrative Court of March 2001 (Catalogue n° 401/00) the Inspector General is an authority neither for controlling- nor for supervising the correctness of applying substantive and procedural law in the cases falling under other authorities, services or courts, whose judgements are subject to assessment in the course of instance or in any other way determined by relevant procedures.

Up to now the Inspector General for Personal Data Protection is the only authority in the Polish legal system who is competent to handle complaints concerning personal data protection.

Poland is invited to clarify in how far data files under the Chief Commander of Police are an exception to the competences of the DPA.

Experts consider it crucial that in case of the SIS, whatever format will be chosen for SIS II, the DPA's full competences remain and that SIS (II) is not considered an exception as foreseen in art 43. Poland 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.

If the data subject is refused by the SIRENE bureau to access to his personal data, to correct or to delete it, the data subject should be able to appeal to the independent supervising authority. This procedure is in conformity with Convention 108 of the Council of Europe, which wouldn't be the case if the right of appeal were granted before the Minister of Internal Affairs.

It appears that on average, the DPA handles some 1000 complaints a year.

When the DPA is not in a position to disclose data, which will for instance be the case in the future with Art. 99 alerts, an appropriate answer is chosen on a case by case basis. An example of this could be: *"There is no information about you that can be disclosed".*

Requests for information are free of costs, except for a fiscal stamp. However, requests introduced from abroad do not require such a stamp. The DPA informed the experts about the methods of submitting complaints to the Authority (one of the methods mentioned was the possibility to submit requests by way of electronically signed email messages). The experts nevertheless remained somewhat confused about the DPA's statement that it could also deal with requests submitted orally.

According written explanation of the Inspector General the Polish administrative procedure is subject to the principle of proceeding in writing. Pursuant to Article 63 paragraph 1 of the Code of Administrative Procedure, applications (requests, explanations, appeals, complaints) may be filled in writing, by telegraph or by teletypewriter, fax, electronic mail or a form posted on the website of the competent authority of public administration allowing for entry of data into the information system of this authority and orally to the minutes. Thereby the application for access to one's personal data, their rectification, erasure as well as complaints on unlawful processing of personal data may be lodged also orally. The law prescribes, however, that the application filled orally should be entered into a written minutes which consists a part of files of the case. The applications filled orally also have to meet some conditions specified by the law (indicate the person of the applicant, his/her address and the request as well as contain a signature of the applicant). Application filled orally to the minutes institutes a proceeding in the result of which the authority being filled with the application has to present its position in writing (in the binding administrative decision) on the request contained in the application. The Polish law generally does not allow presenting such position orally. Furthermore, it needs to be underscored that the procedure of lodging complaints and filling applications orally, due to the requirement obliging the applicant to sign the minutes in which his/her application was recorded, does not allows for filling the applications by phone. Pursuant to the principle of proceeding in writing all materials collected in the course of proceedings (e.g. explanations) must be recorded in writing.

3. SUPERVISORY ROLE (INSPECTIONS)

In the last five years the Polish DPA has performed more than 1000 inspections, leading to almost 600 drafts of administrative decisions presented to the Inspector General for Personal Data Protection to be signed. From the moment the draft decision is signed by the competent authority the document becomes an administrative decision, i.e. legally binding imperious adjudication of the authority issuing the decision. The charges against the administrative decision are raised by the data controller in the course of instance supervision (in this case in the form of request to reconsider the case) and subsequently before administrative courts.

The inspections also revealed 089 notifications of suspicions that crimes have been committed. The inspection visits, which are unannounced, have included inspections of the Chancellery of the Prime Minister, ministries, the Supreme Chamber of Control, courts, public prosecutors offices, the Police Headquarters, revenues, the National Remembrance Institute, the Spokesman of the Public Interest Office and others.

At the request of the experts, a copy of such an inspection report has been made available to verify - not so much the content of one specific inspection - but the methodology of inspection applied. A study of the report showed the inspection to be very detailed. The inspection team was given access to the physical premises, to a number of official documents and to a considerable range of officials at different levels of authority in the inspected institution. The report indicated that a number of meeting reports were made following interviews with responsible officials and later served as a valuable source of input in the drafting of the inspection report. Despite an overall positive impression, the inspection report clearly lacked concrete conclusions and recommendations for improvement. The report constituted a factual overview of the current state of the inspected institution.

According to written information from the Inspector General, the report of the inspection is not an administrative decision yet, but constitutes evidence (description of facts) on the basis of which the assessment of the compliance with data protection rules is carried out and subsequently the administrative decision can be issued.

The inspectors prepare in the form of an internal memo conclusions of the inspection which are the basis for institution of the administrative proceedings concluded with the issuance of legally binding administrative decision which is delivered to the data controller subject to the inspection. In this decision the Inspector General orders (not recommends) to restore within the fixed time limits a proper legal state. Simultaneously it needs to be noted that pursuant to Article 18 paragraph 1 point 3 and 5 of the Act on the Protection of Personal Data the Inspector General for Personal Data Protection may by the means of administrative decision order to apply additional measures protecting the collected personal data or to safeguard the data from the organisational (e.g. the obligation to introduce the mechanism for control of the access to the premises in which personal data are being processed, tightening the procedure of granting access rights and the scope of authorisation to process personal data) and technical (e.g. application of a higher security level by means of application of additional security measures against uncontrolled access from the information network, enhancing the authentication measures, introduction of the obligation to make additional backup copy, introduction of physical safety measures etc.) point of view.

The DPA does not have the capacity to impose fines, although a proposal for such a legislative change has once been tabled.

The DPA has however the capacity to order changes - or more in general to restore the proper legal state.

Notifications on crime are forwarded to public prosecution bodies. Experts were told that in cases of inspection of specific entities, e.g. controllers of data constituting a state secrecy because of state defence and security, protection of life and limb of people, property or public safety and order, the limitation to the right of inspection is limited to the fact that the inspector carrying out the inspection has a right to examine the data file containing personal data only through an intermediary being the representative of the organisational unit subject to control.

It remains unclear whether the DPA has the power to order changes to be made in technical systems. If for instance the DPA is of the opinion that a computer data base should be governed by more stringent technical rules, it is unclear if it can impose its views, or only try to convince the controller/owner of the database.

Both parties, the DPA and the controllers, have the right to contest decisions or the improper implementation of the decision to administrative courts.

4. TECHNICAL SECURITY REQUIREMENT

Experts were informed about the envisaged legal framework, the structures and the technical security characteristics at the SIRENE office.

Despite the fact that in the scope of coming changes the intention was mentioned to draft a national Act on SIS/SIRENE and relevant regulatory provisions, as mentioned in the answers on the Questionnaire 9820/1/05/REV 1 ADD 1, apparently no start was made to draft such legislation, nor was a Schengen implementation group formed, which would include the DPA, so as to share information about changes to come with all involved parties.

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, the technical security measures and the future System user guide. The implementation however seems to be far from decided yet and some answers given in the Questionnaire 9820/1/05/REV 1 ADD 1 have become outdated and do not reflect reality.

5. DATA PROTECTION IN RELATION TO VISA ISSUANCE

The DPA has at this stage has not been involved in the preparation at the Ministry of Foreign Affairs for the connection of the Consulates to the art. 96 database, although the DPA has performed an inspection at the Ministry of Foreign Affairs.

Experts recommend that the DPA would be more proactive in the work going on in the preparations to the inspections of the Consulates.

The only efforts made until now deal with the welcoming of some experts from other Ministries who are employed as trainees at the DPA in order to be made aware of Data protection issues when returning to their Ministry of origin.

It is particularly recommended that the DPA would consider paying a visit to a consulate and to promote 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 SCHENGEN visa application.

Moreover, the DPA should consider whether it would like to proactively offer to visa applicants, whose application has been turned down, the possibility to check in the system whether it does not contain erroneous data.

6. INTERNATIONAL COOPERATION (COOPERATION WITH OTHER DPA)

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

Experts noted in particular the efforts made to develop common experience and cooperation among the Data Protection Commissioners of Eastern and Central Europe, both current EU member states and acceding states.

7. PUBLIC AWARENESS (INFORMATION POLICY)

Despite an active press-policy, the DPA has not yet envisaged plans for a campaign accompanying the implementation of the Schengen acquis in 2007. Much information is already made available through a website, which is available in Polish, English and French.

Additionally, the DPA performs training sessions carried out in the premises of data controllers.

The DPA should verify and possibly assist the Police and the Border Guard with the development of their websites, in particular with the rights of citizens in relation to Data protection.

8. CONCLUSIONS AND RECOMMENDATIONS

General conclusion

1. The experts are confident that the Data protection rules in Poland will comply with the requirements of the Schengen acquis, once a satisfying follow-up has been given to the recommendations mentioned below. Poland 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 and updating the answers given in the Questionnaire 9820/1/05/REV 1 ADD 1.

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. Such additional legislation should in any case ensure that the DPA's competences are not restricted by considering the controller of data managed in the future SIS as a controller of data constituting a state secret because of state security, protection of life and limb of people, property or public safety and order.

On the implementation

3. It is recommended that the Bureau of the Plenipotentiary of the Government for Preparation of the Authorities of Public Administration to the Co-operation with the Schengen Information System and Visa Information System, should closely work together with all interested and relevant partners (DPA, Police, Border Guard, Consular services + other authorities) to share information and to monitor closely the work in progress.
4. There is a need for closer co-operation between the Bureau of the Plenipotentiary and the Polish Data Protection Authority.
5. Poland is invited to develop plans for a campaign accompanying the implementation of the Schengen acquis in 2007.

On the functioning

6. 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.

7. As an outcome of supervisions, it is recommended to clearly state concrete conclusions and recommendations for improvement.

8. It is recommended that the DPA be more proactive in the work going on in the preparations to the inspections of the Consulates.

9. The DPA should, while performing the inspections scheduled for 2006 and on, 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. Verify and possibly assist the Police and the Border Guard with the development of their websites, in particular with the rights of citizens in relation to Data protection.