Council of the
European Union

Brussels, 16 July 2018
(OR. en)

13434/1/02
REV 1 DCL 1

SCH-EVAL 30
COMIX 599

DECLASSIFICATION

of document:	ST 13434/1/2002 RESTREINT UE
dated:	3 December 2002
new status:	Public
Subject:	Report on the Schengen evaluation of the Benelux countries - 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 December 2002

13434/1/02 REV 1

RESTREINT UE

SCH-EVAL 30
COMIX 599

NOTE

from :	the Schengen evaluation committee
to :	the Schengen Evaluation Working Party
Subject :	Report on the Schengen evaluation of the Benelux countries - Data protection

Report on the Belgium Data Protection visit

0. General comments

The Commission de la vie privée - Commissie voor de bescherming van de private levenssfeer - is the Belgian national supervisory authority for data protection in as referred to in article 114 of the Schengen Convention.

The Commission is assisted by a secretariat, which consists of approximately 25 persons. About $^{2}/_{3}$ of the staff has an academic level. Legal advisers and it-experts are employed by the Commission.

The expert team has decided to focus on the following sensitive areas.

1. The right of access of citizens to their files

The Belgium law grants to the Belgian Data Protection Authority (DPA) the right to supervise, correct or delete data in connection with the Schengen Information System at the request of a citizen.

This has actually happened only in a limited number of cases, no more than 10 per year since 1995, with a brief peak in 2000 and 2001. This peak might be explained by a public awareness campaign, launched by the DPA. Another factor explaining the peak could be the that fact that Belgium co-hosted the EURO 2000 and in that period took measures strengthening the border controls. Despite the limited value of statistics on such small numbers, it appears that a majority of access inquiries is linked to airport or border control or to visa denial.

The experts were puzzled by the fact that the intervention of the DPA will in no case lead to transparent information for the requesting citizen. The Belgian legislation excludes the possibility to give any information to a citizen about his/her police file, except for a sentence saying that everything is in compliance with the obligations under the law. This has the consequence that a citizen cannot really prove that information is incorrect, or in case of a visa demand, the applicant will not be informed if he later might have a chance for a successful application. The DPA informed the expert group that the lack of transparency vis-à-vis the individual seeking access to his own data, at least as regards to police files would be raised before to Belgian Parliament in October.

A positive fact is that the DPA is informed of the outcome of every access request by a citizen. It would be an asset to publish every year the number (or the rate) of corrections or deletions.

Although the DPA could not provide exact figures it estimated that in ¼ of the cases, data had been deleted.

The Belgian DPA showed a willingness to improve the system in many respects. It has engaged in efforts to distribute the Schengen SIS brochure at airports and at seaborders.

2. Supervisory role

The DPA would like to see the DPA attached to the Belgian Parliament. This would render more independence from the Ministry of Justice (especially budgetary independence). This would - in the opinion of the DPA - in many ways benefit the DPA and give it status that in many ways is comparable to the one exercised by the Ombudsman-institution.

The last SIS-inspection took place in 1999. The DPA then discovered serious problems related to the physical security of the premises of the SIRENE bureaux and inadequate screening of personnel.

The problems regarding physical security are still unresolved.

When asked why no inspections had taken place since 1999 the DPA referred to the fact that the Belgian Police are undergoing a major reorganization and to lack of staff within the DPA.

The expert team noted with some concern that the Belgian DPA - when doing SIS-inspections - only can rely one legal adviser with an expertise of the Schengen Convention and three IT specialists. However the IT-specialists were apparently involved in many other tasks. The experts doubt if the authority has sufficient trained staff to perform its functions as national supervisory authority for SIS.

3. The rules on logs

Article 103 of the Schengen Convention states that on an average every tenth transmission of personal data must be recorded.

It appears that in Belgium 100 % of the queries in the N-SIS are logged. It is important to ensure not only that 100 % of the queries are logged, but also that it is possible to find out who queried the database, at what time, and for what purpose the query was done.

The DPA could not provide more detailed information on the specific log files. This was noted with some concern by the expert team.

4. Cooperation with other Data Protection Authorities

In the few cases where it was necessary to cooperate with other data protection authorities to the cooperation was satisfactory, though mainly due to interpersonal relations. Generally speaking the cooperation with the French and German authorities are working well, whereas it is the opinion of the Belgian DPA that the cooperation with the Italian authority certainly could be improved. In the relation with Germany the Belgian DPA noted that both data protection authorities have different views on the grounds for inclusion of German alerts in the SIS when the alerts concern asylum seekers whose application have been turned down in Germany, but who had afterwards obtained the legal right of residence in Belgium.

5. Visa applications

The Belgian DPA has no experience with requests for deletion or correction, in relation to visa request. Given the fact that another data protection authority (the CNIL in France) mentioned that about 20 % of the alerts had to be corrected or deleted and that these data originated by large not only from France, the Belgian authorities could assume that a comparable percentages of alerts is possibly erroneous.

The Belgian DPA states that in all Belgian consulates, visa application are dealt with by Belgian staff and that there are no problems related to data protection issues at the consulates. (Note: This is also the conclusion of the (adopted) report on visa).

6. Other topics

- The experts were surprised to hear that the Belgian DPA disagrees with any way of searching in the SIS by Police officers other than by typing in the entire name, date of birth etc. The reason for that is that in their view this is a solution that better protect the 'non-guilty' individual. To the experts this is a slow non reliable method of searching compared with the one in use in almost all other Member states. Experts are of the opinion that search algorithms are very effective to ensure a 100 % result on every alert. It allows too to give time to the police officer to communicate with the controlled person. It seems particularly odd if one considers that searches into Belgian national data files allow phonetic searches or abbreviations.

- It was interesting to notice that the Belgian authorities would welcome a European recommendation defining both how the access of an individual should be organized, direct or indirect, but maybe even more importantly, whether transparency should be granted for police files or not. It should be recalled that even in the case of direct access, some groups, like visa applicants who have been turned down, will always need the assistance of a DPA.

7. Overall conclusions

The expert team concludes that in general the data protection level in Belgium is quite satisfactory considering the constraints of national law and that there are no major problems in the procedures implemented and the way in which the role of the Belgian DPA is carried out.

However, the expert team wishes to make the following recommendations and comments:

1. It should be considered to perform a new SIS-inspection and to address the problems concerning physical security
2. According to the Belgian DPA the authority is partly understaffed which inter alia means that SIS-inspections are not carried regularly - this is - in the opinion of the expert team - a significant problem

8. Final remarks

The expert team would like to thank the Belgian authorities for the good cooperation, for giving information to and answering questions from the team and for the providing of English interpretation during the visit.

* * *

Report on the Data Protection visit to the Netherlands

0. General comments

The Dutch Data Protection Authority (DPA), founded in 1989, performs its task on the basis of the Dutch Data Protection Act and a specific Police Files Act.

The DPA has a board of 3 members and a staff of 60. About 50 % of the staff has an academic level. Legal advisers and it-experts are employed by the DPA.

Ahead of the visit the DPA had given detailed answers to a questionnaire which made a good basis for the work of the inspection team. The expert team has decided to focus on the following sensitive areas.

1. The right of access of citizens to their files

The right of access of citizens to police data is - according to Dutch law - of a direct type. This means that citizens should ask the police directly to check, correct or delete certain data. This procedure is commenced after the data subject has identified himself in writing and paid a sum of 4.50 euro.

According to the DPA it is the estimation of the Dutch Police that the number of direct requests made to SIS-files will be about 200 in the year 2002.

The Dutch DPA is in general initially not involved in these requests. It deals with an average of less than 10 cases a year regarding SIS-access. As the right of access is exercised directly through the police, a lot of the cases involves only sending the requests through to the police.

According to the Dutch Act on Police files, the Police is - as a starting point - supposed to inform the person about the content of his/her file. There are however exceptions from this. According to the Act on Police Files information on files can only be given orally.

When the DPA sends an access request through to the police it asks to be informed on the outcome of the request. The DPA informed the team that such information almost never is communicated to the DPA by the police.

The Dutch DPA has only the power to act as a mediator in cases about access to police files. Thus the DPA can never make a final ruling and order the police to act in certain way - for instance provide information to the subject which was not given initially. A data subject unhappy with an answer form the police can although challenge the decision in a court of law.

The experts is of the opinion that one positive element of the Dutch system is that the requesting person is informed about the content of his file. However, the experts were somewhat puzzled by the fact that the DPA is not informed about the results in the majority of cases i.e. the cases where the decision of the police not subsequently is brought before the DPA asking to exercise their power as a mediator. It is unclear whether this system, which is based on great confidence in the accuracy of data, could be seen as an example or that a feedback and evaluation through an independent Data Protection Authority offers more legal security. Given the fact that another DPA (the CNIL in France) mentioned that about 20 % of the alerts had to be corrected or deleted and that these data originated by large not only from France, the Dutch authorities could assume that a comparable percentages of alerts is possibly erroneous. It might be recommendable to have the Dutch police report, i.e. once a year, on the requests it has received and the follow up given to it.

The expert team noted with great satisfaction that the DPA has published an information folder on SIS[1] and a pamphlet on general guidelines on right of access and has published information concerning the right on the website of the DPA.

[1] "The Schengen Information System"

2. Supervisory role

The DPA has been designated as the Dutch authority as meant under article 114 of the Schengen Convention.

Besides the supervisory role of the DPA the authority acts as an advisor on data protection issues in general and especially on new legislation. The DPA is also involved in international work. The DPA emphasizes heavily on public awareness on data protection issues in general and tries to promote the idea of stimulating self-regulation.

The Dutch DPA has performed a general inspection of the Dutch part of SIS in 1997 and a follow up audit in 1999. It appeared from this re-audit that important progress had been made, although there was still major issues on physical and logical authorizations (security of the premises) which remained unresolved.

The experts consider this way of auditing and follow up in principle very useful.

The experts noted with some concern that a follow up audit concerning the remaining shortcomings was not carried out and that a new inspection is not planned. This is mainly because of lack of trained staff - especially it-experts within the DPA.

The DPA has informed the experts that the Dutch government recently has announced that it will introduce an obligation for the Dutch police to have their files audited on a regular basis.

3. The rules on logs

Article 103 of the Schengen Convention states that on an average every tenth transmission of personal data must be recorded.

It appears that in the Netherlands every transaction is logged.

The team notes that it is important to ensure that not only queries are logged, but also that it is possible to find out who queried the database, at what time, and for what purpose the query was done.

The DPA could not provide more detailed information on the specific log files. This was noted with some concern by the expert team. [2]

4. Cooperation with other Data Protection authorities

In the few cases where it was necessary to cooperate with other Data Protection Authorities to obtain supplementary information on an alert, this cooperation was satisfactory.

5. Visa applications

The Dutch DPA has very little experience with requests for deletion or correction, in relation to visa request. Given the fact that another data protection authority (the CNIL in France) mentioned that about 20 % of the alerts had to be corrected or deleted and that these data originated by large not only from France, the Dutch authorities could assume that a comparable percentages of alerts is possibly erroneous. However the expert team has noted that the information campaign about the SIS[3] has been launched in the Netherlands. Furthermore the team noted that the DPA was actually not sure whether Dutch legislation would apply to the territory of Consulates. The team recommends that this is investigated. [4]

[2] Additional comment received from the Dutch Data Protection Agency subsequently to the visit:
"According to the regulations for NSIS and SIRENE it is compulsory to log data concerning the person who queried the database, at what time, and - in almost all cases – for what purpose the query was done. The purpose of the query is not logged when direct access is provided according to article 101 of the Schengen Convention."
[3] Cf. footnote 1
[4] Additional comment received from the Dutch Data Protection Agency subsequently to the visit:
"Dutch legislation is applicable at the territory of Consulates."

6. Other topics

It appeared from the answers to the questionnaire that in Schiphol airport there is a kind of duplication of the N.SIS database, which only contains some information of wanted persons and issued and blank documents. This is apparently meant for performance reasons. The question is whether this system with an "incomplete" database at Schiphol airport, imbeds a potential risk for missing hits due to the incomplete nature.

The DPA was not aware of the issue raised, so they did not take a position on that. [5]

7. Overall conclusions

The expert team concludes that in general the data protection level in the Netherlands is quite satisfactory and that there are no major problems in the procedures implemented and the way in which the role of the Dutch Data Protection Agency is carried out.

However, the expert team wishes to make the following recommendations and comments:

1. A possible recommendation to the Dutch authorities would be to organize a system of feedback on deletions/corrections to police files, in order to get a complete picture of the accuracy of data.
2. The team is of the opinion that the unresolved problems with security discovered on the N.SIS inspection must be resolved and that this issue must be given due attention by the DPA.
3. The expert team recommends that the Dutch DPA turns its due attention to the use of SIS by Dutch consulates and embassies. In this connection the use of logs is of specific interest.

[5] Additional comment received from the Dutch Data Protection Agency subsequently to the visit:
"The incomplete data base which is meant is called Ken0-key data base. At the border check on Schiphol only some data of passengers are used for searching the Ken0-key data base (first letter of the given name, first four letters of the surname and the year of birth). The data in the Ken0-key data base are automatically copied from the N.SIS. An automatical control function has been installed. For every hit in the Ken0-key data base, the N.SIS is always queried for the full data stored. This doesn't happen while the passenger is waiting in the line. The passenger is directed to a waiting room where a separate check in the N.SIS will be executed.
The incomplete nature in the Ken0-key data base is covered. For example data on vehicles are not stored in the Ken0-key data base, which should not be a problem at Schiphol airport because no vehicles are passing there."

8. Final remarks

The expert team would like to thank the Dutch DPA for the good cooperation and for giving information to and answering questions from the team. Members of the team very much appreciated the written information provided by the DPA.

* * *

Report on the Luxembourg Data Protection visit

0. General comments

It is important to notice that a new data protection act[6] that will transpose Directive 95/46/EC[7] in Luxembourg legislation has been adopted and will enter into force on 1 December 2002.

The act sets up an independent national supervisory Commission (Commission nationale pour la protection des données). Another special supervisory authority has the exclusive competence when dealing with police files.

The national Commission is a public authority acting under the structure of an "établissement public". According to article 34 of the law, the commission has financial and administrative autonomy. It fulfills its missions in total independence.

The special supervisory authority is composed by two members of the national commission and the public general prosecutor or his delegate as chairman. The general public prosecutor is a member of the judicial power.

The structure chosen, an "Etablissement Public", represents the highest level of independence in the Luxembourg judicial tradition, which is emphasized by the authority given to the general prosecutor. The National Commission will have its own budget and sufficient staff.

The expert team has decided to focus on the following sensitive areas.

6 Loi du 2 août 2002 relative á la protection des personnes á l'égard du traitement des données á caractére personnel

7 Directive 95/46/EC of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data

1. The right of access of citizens to their files

The data protection authorities in Luxembourg (DPA - both the present and the ones envisaged in the new act) have the exclusive competence to handle requests for access to the SIS.

Until now the number of requests regarding access to SIS files has been extremely low; approximately one per year. The national authority receives these requests both directly or through various other channels**.** The low number of requests may be explained by the size of Luxembourg and it's population, and/or by the fact that Luxembourg has not distributed a leaflet on the SIS and the right of citizens. This appears to be a result of a reluctance on the part of the administration to fund such a campaign rather than on the part of the authority. The creation of a new authority with an independent budget may allow this issue to be addressed. It could be considered useful to increase public awareness about the SIS - possibly at the time when the new act will enter into force.

Another explanation of the relatively low number of requests regarding the SIS could be that as in Belgium the legislation in Luxembourg explicitly exclude rendering any information to the data subject concerned. Because of this a citizen can not be informed of the content of his file. He will only be informed that no information – if any – is being processed within the SIS contrary to national law or the Schengen Convention. As a result of this a citizen cannot prove that personal information regarding the subject is incorrect/inaccurate, or in case of a visa application the applicant will not be informed if he later might have a chance for a successful application.

2. Supervisory role

Once or twice a year an inspection of the N.SIS and/or the Sirene office is conducted by the DPA. In the past some problems relating to the physical security were discovered, but these problems have been handled in a diligent way by the police.

The expert team was very pleased to note that in Luxembourg any authorized person queering the SIS must choose from a drop down list the reason for his or her query of the system (e.g. “border control”). This information is then stored in the log-file.

As a supplement to the on-site inspections a computer expert acting on the behalf of the DPA – using a specially designed it-tool - examines the log-file for “suspicious” behavior (e.g. an unusual amount of queries within a short period of time). This is done every 3 months.

3. The rules on logs

Article 103 of the Schengen Convention states that on an average every tenth transmission of personal data must be recorded.

It appears that in Luxembourg every transaction is logged.

The team notes that it is important to ensure that not only queries are logged, but also that it is possible to find out who queried the database, at what time, and for what purpose the query was done.

As mentioned above the authorities keep supplementary information concerning the reason for queries in the log-files.

Log-files are recorded on CD-ROMs. The files on the CD-ROMs are encrypted and an entrusted person is designated to transport the CD-ROMs from the police to the computer expert who is examining the files. The log-files are kept in a safe.

The logged files contain only the "transaction" and not the content itself. However, it is possible to check afterwards which officer made a query and to verify his motives.

The expert team noted with some concern that the log-files apparently are stored indefinitely. The tapes or CD-ROMs are never destroyed. No explanation for this was given.

The DPA could not provide further information on the specific log files. This was noted with some concern by the expert team.

4. Cooperation with other Data Protection Authorities

The number of cases in which this international cooperation was necessary is insignificant (1 in total). However the cooperation in this case worked out well, mainly due to interpersonal relations.

5. Visa

The DPA was not aware of that any request for changes or deletion in relation with visa application have been made. No such a case has ever been brought for the DPA. The Luxembourg consulates do not use the so-called Benelux CD-ROM, containing the SIS files and designated as a tool for those consulates, which are not linked to their Ministry of Foreign Affairs by electronic communication.

According to the DPA the consulates have the Ministry of Foreign Affairs in Luxembourg check the SIS when handling visa applications. Communication is carried out by encrypted fax.

The expert team was puzzled to note that the number of queries to the Ministry of Foreign Affairs apparently amounts to 20.000 per year.

6. Overall conclusions

The expert team concludes that in general the data protection level in Luxembourg is quite satisfactory and that the Luxembourg data protection authority carries out its tasks in a very diligent and satisfactory way.

However, the expert team wishes to make the following recommendations and comments:

1. It should be considered whether it is strictly necessary not to destroy old log-files
2. It could be considered to launch some sort public awareness campaign regarding the SIS

7. Final remarks

The expert team would like to thank the Luxembourg authorities for the good cooperation and for giving information to and answering questions from the team.

* * *