Journal of Information, Law and Technology

The Schengen Information System in Austria: An Essential Tool in Day to Day Police and Border Control Work?

Stephen Kabera Karanja
Research Fellow, Section for Information Technology and Administrative Systems, Faculty of Law, University of Oslo, Norway.
s.k.karanja@jus.uio.no

This is a **commentary** published on: 22 March 2002

Citation: Karanja S K, 'The Schengen Information System in Austria: An Essential Tool in Day to Day Police and Border Control Work?', Commentary, *The Journal of Information, Law and Technology (JILT)* 2002 (1)
<http://elj.warwick.ac.uk/jilt/02-1/karanja.html>

Abstract

This article discusses the Schengen Information System (SIS) in Austria. SIS is a joint information technology and communication system for exchange of information concerning wanted persons and objects. Its purpose is to allow checks on persons to be made quickly and efficiently at border controls in order to detect criminals and illegal immigrants moving into and from one Schengen country to another. The article is based largely on interviews with key persons responsible for SIS in Austria, supplemented with background material from written literature and legal sources. The purpose of the interviews was to gather information on the functioning of SIS and the implementation of control mechanisms. The general conclusions are that SIS is functioning well and has become an essential tool in day-to-day police and border control work. The control safeguards are also working well. However, there are a number of concerns that need to be addressed, while others are already being addressed. These concerns are discussed in detail as an evaluation of the effectiveness of SIS' internal and external control and safeguards.

Keywords: Schengen Information System, SIRENE, Internal Control, External Control, Schengen Convention, Schengen co-operation, Border Control, Exchange of information, Austria.

1. Introduction: Methodology

The interviews were carried out in Vienna between 26 February and 8 March 2001. The people interviewed were from the Austrian Data Protection Commission (DPC) and the Ministry of the Interior. From the DPC, the deputy data protection commissioner was interviewed, and from the Federal Ministry of Interior, five persons were interviewed in total: the head of the National Schengen Information System (NSIS) and Data Processing Unit, the technical representative to the Schengen Council, a senior officer in the Department of Immigrations, the director of the Austrian SIRENE (Supplementary Information Request at the National Entries), the co-ordinator for data protection, law and order and, finally, person responsible for legal, organisation and financial questions in the Data Processing Unit and a national legal representative to the Schengen Council.

The interviews were informal and semi-structured. The interviewees were sent a similar list of general questions in advance, with which they could prepare and orient themselves before the interviews. As it was not possible to substantiate the information collected through independent sources, given the sensitive nature of the system itself, a standard list of questions was used for cross checking and verification purposes. Consequently, it was easier to substantiate information received during an earlier interview with that of a later one. Another advantage of using general questions was that it encouraged interaction with the interviewees. The objective was to give them leeway to express themselves freely and in-depth. During the interviews, the general questions were supplemented with more specific oral questions posed by the interviewer. These questions were aimed at eliciting further information, in particular information relevant to the role of the specific department being interviewed. The general questions covered a range of issues such as

Schengen legislation and documentation, functioning of SIS and SIRENE, data quality and security, data modelling, role of SIS in the Schengen co-operation, the relationship between SIS and other cross-border systems. Following each interview session, the interviewer documented the interview as a written report, from notes taken during the interview. Later, the written reports were sent to the interviewees for verification and comment. In some cases, additional verification questions accompanied the reports. Out of a total of five reports sent, response was received for three documents with clarification and additional comments. In general, the interviewees were informative, open and candid in their responses.

2. Background Information

Austria joined the Schengen co-operation in 1995 but did not begin to implement the Schengen Convention until 2 December 1997. The two year delay may seem long, especially as Austria already had a data protection legislation, dating from 1988. However, other legislative, technical and border control conditions needed to be fulfilled before implementation could commence. The Schengen Convention had to be incorporated into the national legal system, the Schengen Information System established, and external border controls improved. The issue of external border control was especially thorny for Germany. Austria's Schengen external border with the Czech Republic, Slovakia, Hungary, Slovenia , Switzerland and Liechtenstein is 1,200 km long. Germany was concerned that Austria might not be able to fulfil the conditions for external border control, and insisted that Austria effectively control its external borders before beginning to implement the Convention. In the interview with a representative of the immigration authorities, it transpired that Austria had used ATS 3 billion to enhance control along its external borders. Over 6,500 new personnel had been deployed along the external border, new technical equipment bought, and SIS IT infrastructure laid down in an effort to comply with Schengen external border control conditions.

3. Schengen Information System

3.1 General

SIS consists of two main components: the national systems referred to as the national SIS (NSIS), located within the territories of each of the Schengen Contracting Parties, and a central technical support system known as the Central SIS (CSIS), situated in Strasbourg, France, (Article 92). NSIS enables designated national authorities to carry out searches in SIS. CSIS ensures that data files of the national sections are updated and kept identical at all times by online transmission of information.

SIS is the most important technological compensatory measure in the removal of internal borders in the Schengen co-operation. It is a fundamental requirement for implementation of the Schengen Convention. No country may commence implementation of the Convention before SIS has been established. The persons I interviewed at the Ministry of the Interior were of the opinion that SIS plays an important role in crime and border control. Hence, it has become a very important tool in day-to-day police work. To illustrate this, one interviewee referred to the first case to be solved through SIS in

Norway. He emphasised that, had it not been for the Schengen co-operation and SIS, such a quick arrest could not have been possible. My experience in crossing the Schengen external border between Austria and her two non-Schengen neighbours - Hungary and Slovakia - confirms that SIS has indeed become an important tool in border control work.

3.2 Establishment of the System and Data Modelling

As the responsibility for establishing the national part of SIS - NSIS - is left to individual Contracting Parties (Article 92), countries have come up with different technical and data modelling solutions. The question regarding the establishment and data modelling was aimed at finding the path the Austrian authorities had followed and whether it had been influenced by other Contracting Parties' solutions.

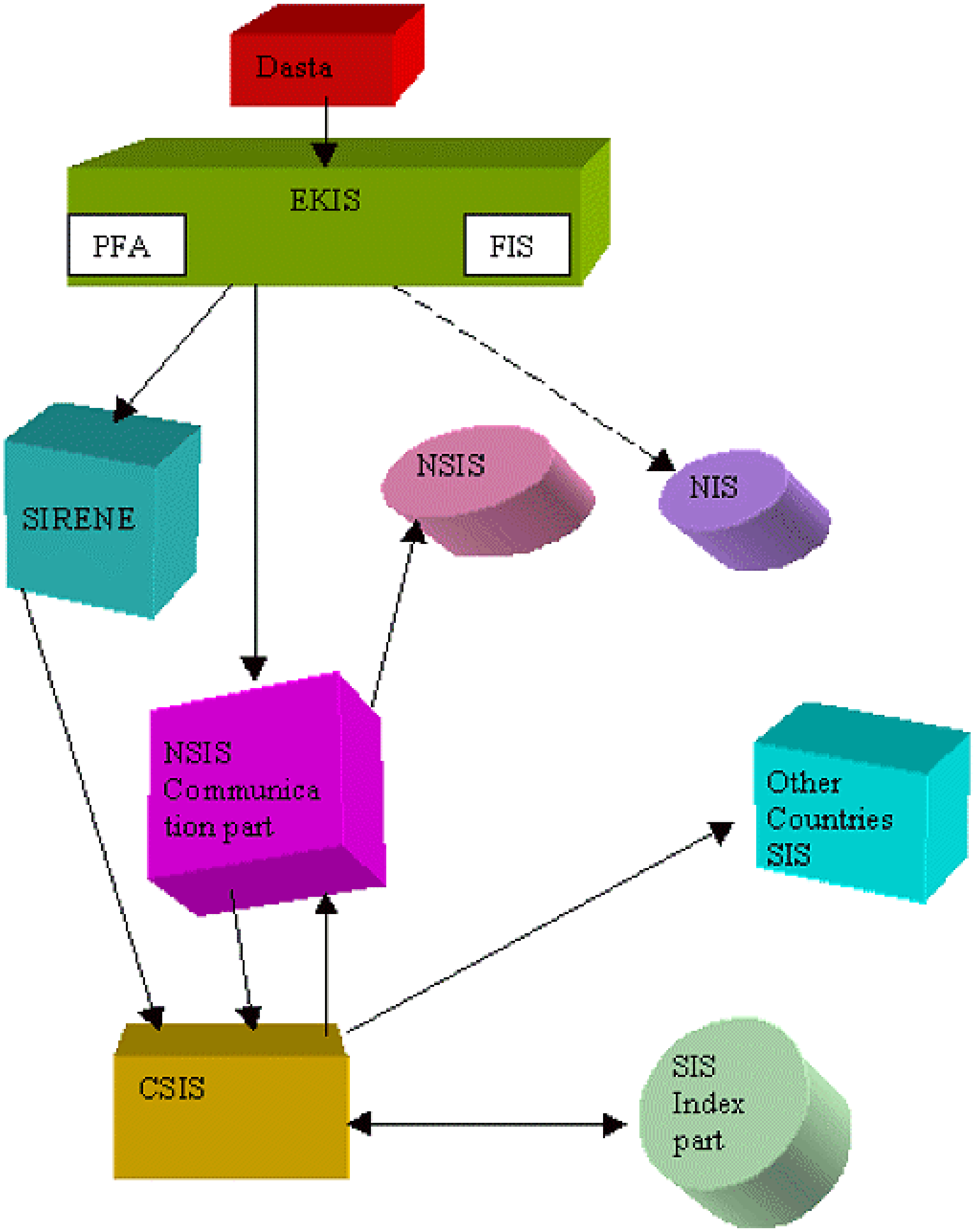
The findings reveal that, in Austria, the Ministry of the Interior has responsibility for the operation of SIS and, therefore, undertook the task of establishing the system.Other government ministries were involved in the establishment efforts, however, namely the Ministry of International Affairs, the Ministry of Justice and the Ministry of Finance. The Data Protection Commission, though not directly involved, was often consulted, especially regarding data protection matters. As for the technical aspects, the establishment of NSIS was the result of the work of the Ministry of the Interior's Electronic Data Processing (EDP) -Centre, in co-operation with IBM. It was emphasised that the Austrian solution had been a success and has been exported to the Nordic countries, particularly Norway.

It was also emphasised that the Austrian NSIS is based on pre-existing national infrastructure. However, it was not developed in isolation. The team involved with implementation studied other countries' solutions, in particular those belonging to Spain, Portugal, the Netherlands and Germany, most of whom operate different systems.

As regards data modelling, the Austrian team did not need to create a new data model and design as this was already stipulated in the Schengen Convention. Their task was to follow the Schengen provisions, indicating which data is to be registered and the reasons for registration. In addition, a dictionary for storage that directs how data is to be stored already existed. Therefore, it was not necessary to develop a separate SIS data map, as most of the data that can be registered under the Convention had already been stored in the national information system (NIS). As SIS is largely an index system and database that stores basic data for purposes of search only, data is not stored in relation to categories. For details of data stored in SIS, one has to consult the supplementary data system - SIRENE.

3.3 The Functioning of the SIS

The question regarding the functioning of SIS was necessary in order to illicit information on the process which data follows: from the decision to register, through to when the data is ready for search, and how long this process takes. The aim was also to find out about the technical and organisational relationship between SIS, NIS and SIRENE. The relationship between SIS and SIRENE has been contentious, with some claiming that the systems are one and the same, and others that the systems are separate, both technically and organisationally. The confusion arises because SIRENE is not included in the description of the components of SIS in Article 92 of the Schengen Convention. In addition, the Convention does not refer explicitly to SIRENE.



PFA - Criminal Register
FIS - Foreigner Register
Flow of information

Figure 1: Austria: The Technical Aspects and Functioning of the NIS and SIS

The diagram above (Figure 1) was used during the interviews to answer the question and clarify the confusion. It represents the flow of data and the technical and organisational aspects of SIS in Austria.

The police, immigration authorities, customs services and courts may enter information into SIS. The process of entering data into SIS starts at the police stations. Here, police officers at the first level of criminal police authority prepare an EKIS (national system for criminal investigation) document for entry into the national criminal system. The document is then transmitted to a data station (DASTA), which is a second level security authority (*Sicherheitsdirektion*). At the DASTA, the data is entered online by the staff into EKIS. If the EKIS document contains a special indicator for SIS relevant data, special software filters the data set from the EKIS file and communicates it to a specific file of NSIS, which is then communicated by special software to CSIS. Where the SIS data set is relevant to Article 95 (extradition) or Article 99 (discreet surveillance), it is first communicated to SIRENE and from there onto CSIS. CSIS, after indexing the data, distributes it to NSIS in all Schengen countries, including the NSIS in the reporting country. Once t distributed, the data is searchable. The whole process takes only 3 minutes to complete, which means, therefore, that SIS is very up to date. The same search query is send both to SIS and the national system in Austria. This is because a national search is not only a SIS search, as it also involves a search in the national system. The explanation given was that if this was not the case, persons not registered in SIS would escape detection because a negative hit in SIS does not necessarily mean that a person is 'clean'. Searching the national system may reveal other information, as a person may be registered in the national system but not in SIS.

As shown in the diagram, NSIS, SIRENE and NIS are all different technical and organisational units (see 5.2 below). Personnel working with these systems are different and the systems are located in different buildings. I had to travel to different locations and buildings to interview representatives of the different systems. As regards data protection and data security, keeping the systems separate is desirable so that any data protection problem affecting one system may not necessarily spill over to the other systems.

3.4 Access to Data in the System

Access to data in SIS has also been a contentious issue. The Schengen Convention does not set limits to the number of persons with access authority, instead leaving access regulation to the national laws of the Contracting Parties. Consequently, the list of persons with access differs considerably among the Contracting Parties. The question relating to access to data in SIS was therefore aimed at establishing a clear picture of who has access, how many persons have access and how access is controlled in Austria.

According to the Schengen Convention, data in SIS can be searched and accessed by authorities designated by the Contracting Parties for the purposes of border checks and controls, and other police and customs checks, when carried out inside the country in accordance with national law (Articles 92 & 101). Data entered pursuant to Article 96, relating to foreign nationals, may be searched by the authorities responsible for issuing visas, examining visa applications, issuing residence permits and the administration of aliens, within the framework of the application of the provisions on the movement of persons under the Convention (Article 101(2)).

In Austria, over 30,000 persons are allowed access to the data in SIS using 16,000 stationary terminals throughout the country. This number is not restricted and can be increased as the need arises. In addition, officers on patrol and at external land border crossing points are issued with laptop computers for access to information in SIS. The laptops are equipped with only the most important data, updated on a daily basis. Consequently, the officers cannot access all the data in NSIS. In case of a positive hit, they have to verify the information by radio to the main terminal, as data may have changed since their laptops were last updated. The practice is in line with JSA recommendation regarding copying alerts in SIS.

Foreign missions abroad do not have online access to the SIS. They are issued with a CD containing information necessary to determine whether a person applying for visa should be accepted or not. The result of the query is either a red or a green light. The green light indicates that a visa can be issued if the applicant satisfies all other conditions. The red light, on the other hand, indicates that an objection exists to issuing a visa. In such cases, the officer should verify this and get details from headquarters at home. There are plans for mission offices abroad to submit queries online to SIS in the future. The CD is replaced fortnightly.

3.5 Authorities with Control Responsibilities

Each Contracting Party is responsible for designating which national authorities have control responsibilities (Article 92 & 101). In practice, this means that each Contracting Party appoints the authorities in charge of NSIS. As the Convention does not specify which authorities these should be, the Member States have wide discretionary powers, and one must look at the national scene and legislation to identify the authorities. In Austria, the Ministry of the Interior is responsible for NSIS. It is also the top security organ in Austria. The Ministry has 9 police divisions with 100 police districts below them. Responsibility for control and security follows this hierarchy. Other authorities with control responsibility are Customs and Immigration. The Data Supervisory Authority also has a role to play as a data control organ and appeal body for decisions made by the Ministry of the Interior.

4. SIRENE

4.1 Legal Basis

The issue of the legal basis of the SIRENE is still divided and contentious. Two opposing views seem to exist. The persons I interviewed were also divided on the issue, their views reflecting the two positions. The first position, which is held by the Schengen Member

States and was reflected by the Ministry of the Interior, purports that SIRENE has a clear legal basis in Article 108 of the Schengen Convention. Earlier, in a decision of 1994, the Schengen Executive Committee supported this view by stating that the SIRENE manual contains the legal basis of SIRENE.The second position, which was reflected in the interview with the Data Protection Commission representative and held by the Central Data Supervisory of Schengen (CDSA), claims that SIRENE has no clear legal basis. There is no legal basis in national law and the Schengen Convention does not explicitly refer to the SIRENE. While these two views continue to exist, the issue of the legal basis remains unresolved. However, expectations are that when the second generation of SIS is implemented, rules will be developed to give a clear legal basis for SIRENE.

4.2 Technical Aspects

The creation of SIRENE was meant to give SIS a human interface through which supplementary information on a positive hit in SIS could be exchanged. All relevant case information is exchanged and could include fingerprints and photographs in cases where identification is vital. DNA data are not yet exchanged. For security reasons, SIRENE consists of electronic files only and no manual files. From an organisational point of view, SIRENE is a separate communication system to SIS. In Austria, NSIS and SIRENE belong to different organisations within the Ministry of the Interior. 22 SIRENE officers from the criminal police are working at the Austrian SIRENE office.

4.3 The Process of Exchange of Information

As stated above, SIRENE comes into the picture usually when there is a positive hit in SIS and where supplementary information regarding the hit is required. In such circumstances, a request for information is made to SIRENE. In principle, the request is made to the SIRENE office and not to a particular person. Since the SIRENE office operates 24 hours a day, it is the officers on duty who act when a request is made.

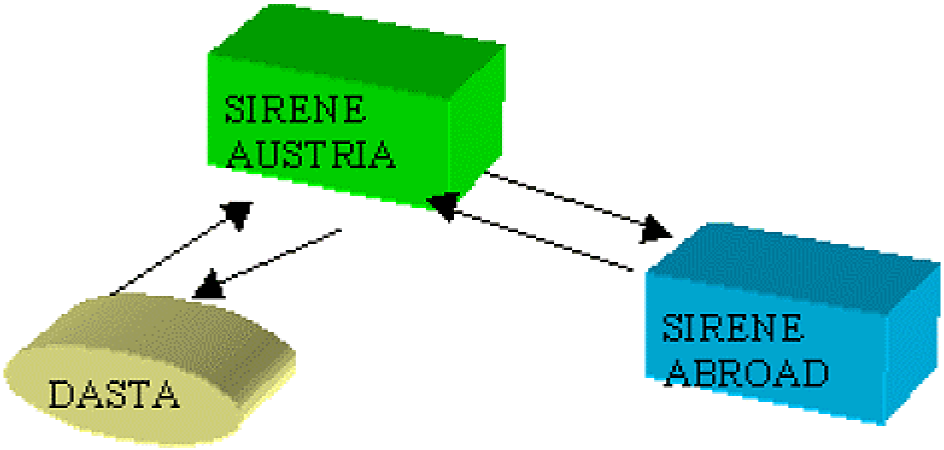


Figure 2: A Hit in Austria

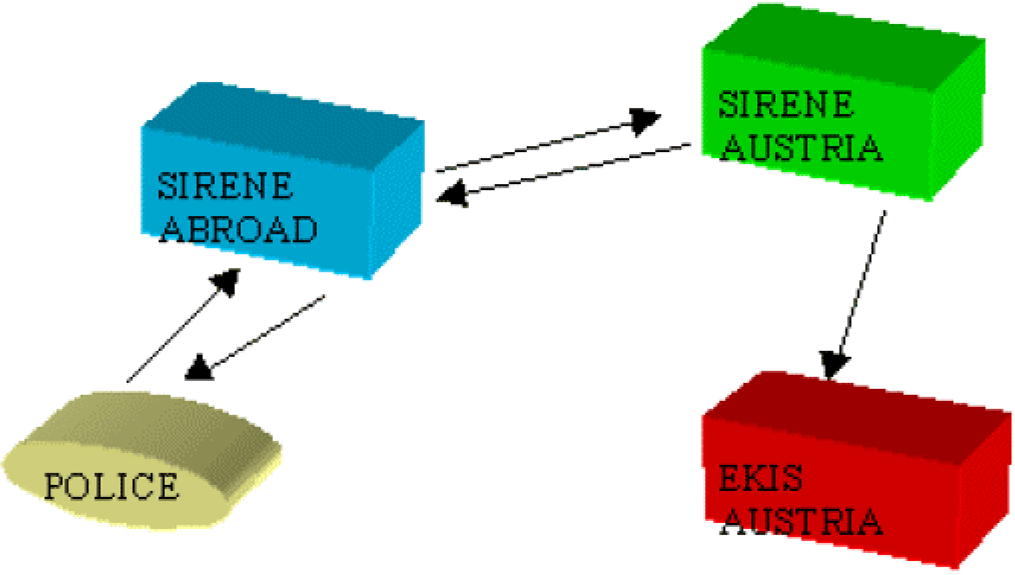


Figure 3: A Hit Abroad

Information is exchanged electronically through standardised forms. For example, a *G - Form* is for a hit and a *Q - Form* for data on usurped identity (a new form for cases where a perpetrator uses the name of a stolen passport as an alias), and so on. There are standardised forms for every purpose, e.g. Article 95 on arrest, Article 96 on foreign nationals to be refused entry, and so on. Where further clarification of electronically transmitted information is required, this may be requested by telephone or additional electronic messages. Supplementary information is supplied on request when there is a hit and further information is required. If a hit occurs in Austria itself, and the authorities require more information, then the request is send to Austrian SIRENE who forwards the request to the SIRENE of the Contracting Party concerned. The supplementary information is then supplied to the Austrian SIRENE and forwarded to the requesting authority (see Figure 2 above). If the hit occurs abroad, the request is made to that country's SIRENE, and then forwarded to the Austrian SIRENE, who retrieves the relevant information and relays it back to the requesting SIRENE to forward to the source of the request (see Figure 3 above). This procedure is applied in all cases, except in cases concerning Article 95. In Austria, supplementary information under Article 95 is prepared at the time of entering a report in SIS. At this time, the necessary information is also prepared and distributed to all foreign SIRENEs. The response time to a request depends on the case. In some cases, it can take as little time as 15 minutes.

5. The Role of SIS on Interstate Co-operation

During the negotiation and signing of the Schengen Convention, a number of documents were designated confidential, making them inaccessible to the public. Even institutions such as national parliaments found it difficult to access documents during the ratification process. The aim of the question relating to Schengen legislation and documentation was to find out which new documents were generated in the process of ratification and incorporation of the Schengen Convention into Austrian legal system, and the extent to which these documents are accessible. It was also necessary to find out about the influence of the Schengen Convention on data protection legislation, especially in the Austrian police sector.

The Schengen Convention is an intergovernmental treaty that requires incorporation into the national legal systems of the Contracting Parties. What emerged during the interviews was that there was no need to enact a new Schengen law, as the Schengen Convention has direct application and legislation status in the Austrian legal system. Austria belongs to the monism tradition. However, some statutes were amended to reflect changes incorporated by the Schengen Convention, for example the Police Co-operation Act. As explained previously, the Schengen data protection provisions did not have a specific impact on data protection regulation in the police sector. Austria has had a long-standing tradition of regulating data processing in police matters. The earlier Austrian Data Protection Act of 1988 applied to police information systems. This has been reflected in the new Data Protection Act of 2000. Consequently, both the Data Protection Act of 2000 and the Schengen Convention apply to data protection in SIS. The Data Protection Act applies only where the Schengen Convention is silent. This is in line with the general rule in the Schengen Convention that states: ‘where the Convention contains no specific provision, the relevant national law of the Contracting Parties applies’.

The long tradition of data protection in police matters is also reflected in regulations. There are no regulations applying to the Schengen specifically. However, data protection regulations and guidelines have been issued that apply to data protection in general. The guidelines are general manuals for input of data into the national information systems, which also would apply to SIS. Apart from these documents, no other publications have been issued. For example, no annual reports pertaining to SIS and no information directed at educating the public on the Schengen Convention has been issued. The only public information on the Schengen Convention was issued in the period preceding the implementation of the Schengen Convention in 1997.

As regards the accessibility of Schengen documents, those interviewed at the Ministry of the Interior, were of the opinion that the documents are accessible. They emphasised that, with the incorporation of the Schengen Acquis into the legal framework of the EU, EU rules on transparency and access to information apply to Schengen documents as well. Nevertheless, Schengen technical documents remain confidential in order to protect the security and integrity of the systems from interference by criminal elements such as hackers.

6. Schengen Legislation and Documentation

When asked their opinion on the role of SIS on interstate co-operation, the interviewees were unanimous in viewing SIS as a positive contribution to interstate co-operation. They pointed out that it has been a very important measure in the realisation of free movement. At first, only few countries were involved in the co-operation, which was outside the EU framework. Currently, 15 countries are members (Great Britain is not a full member and participates in SIS only), of which 13 are EU Member States. It was claimed that this is proof that free movement does work, but it could not work without the security measures undertaken. SIS has been a very important measure in maintaining the internal security of member states and the control of illegal immigration. Searches in SIS have been efficient and have resulted in many positive hits, which have enhanced security and controlled crime and illegal immigration in the Schengen area. The number of hits, both within the country and in the rest of the Schengen countries has increased with time. SIS has played a positive role in these areas.

However, some problems were pointed out which, if solved, could improve the working of SIS. It was said that in Austria, the prosecution and judicial authorities are not making good use of the capability of the system as regards entering data under Article 95. Only about 10% of the system is in use. The national Schengen authorities have initiated dialogue with judicial authorities to try to increase awareness of the system among them.

Another problem relates to the Schengen Convention, which is claimed to be very restrictive regarding the data to be entered in SIS. It was pointed out that this reduces the police ability to deal with crimes that could easily have been dealt with if such information had been allowed. For example, information on stolen car registration plates cannot be registered, although information on stolen cars is permitted. Registration plates are stolen and used on stolen cars to commit robbery or other crimes. If they could be registered, it would be easier to track down stolen cars. This would involve expanding the list of information entered into SIS, and could only be carried out by amending the Convention.

7. Control and Safeguards

7.1 Introduction

Data protection in the Schengen Convention is ensured through a series of rules and control systems. Although rules are important in the protection of data and individual rights, it is the practising of the rules that determines the effectiveness of protection. Control of the application of the rules is what determines the overall effectiveness of the practice. In order to determine how the rules of data protection in Austria are applied, I am going to analyse the control systems that are in use, applying the evidence collected from the interviews. As Cameron (2000) has noted: ‘systems have blends of internal and external controls and remedies’. Below, I will focus on this categorisation of internal and external control.

7.2 Internal Control

Internal control refers to safeguards built into the system to ensure the quality and security of the data, as required under Article 118 of the Schengen Convention. They are a combination of technical, personnel, and organisational controls. *Technical* controls take various forms and are made to ensure that the system complies with data protection rules concerning collection, quality and security of data. The Schengen Information System is an open-loop online system. According to Gregory and Horn (1963, p16), an open-loop online system utilises people for gathering data or carrying out the control instructions, unlike a closed-loop system, which is fully automated at all stages, from data origination through processing back to the implementation of control. People are therefore an important part of internal controls in SIS, especially at the origination of data (collection, conversion and verification) and entry stages. *Organisational* controls refer to the management structures and the responsibilities of both management and staff. For convenience and clarity, I will discuss internal controls through different stages of data processing, starting with the origination of data, entry of data and access to data. Technical controls and personnel involved in control will be discussed for each stage in data processing. Organisational control will be discussed at the end of this section, as it runs throughout all the data processing phases.

7.2.1 Origination of Data

Origination of data refers to three activities: collection, conversion and verification. According to the findings from interviews, police criminal officers of first level collect data for entry into SIS in Austria. They prepare the records for entry into EKIS and flag the data for entry into SIS. Prosecutors and courts collect and prepare data on extradition (Article 95 of the Schengen Convention) for entry into EKIS. Similarly, the immigration authorities collect and prepare data under Article 96, refusal of aliens to enter, for entry into EKIS. The collecting officers are responsible for checking that the data for inclusion into SIS comply with collection of data rules, especially the purpose principle, as stipulated in Articles 95-100 of the Convention. Once the data records are ready, the officers send them to a DASTA. At the origination stage, only human control is performed.

7.2.2 Entry of Data

Both human and technical controls are carried out at the data entry stage for SIS data records. Entry of data into SIS is the responsibility of second level criminal officers at the DASTAs. However, before the data is entered, the officers at the DASTA are required to carry out data verification. Data verification includes checks to determine that the records are in the approved format, convey the correct meaning to the reader, and will lead to the appropriate action. The officers at the DASTA visually control the data record to confirm that it complies with registration rules and, if necessary, correct it. In Austria, this is referred to as the ‘four-eyes -entry’ principle, where two officers visually control the record. When the officers are satisfied that the data record conforms to the stipulated conditions, they enter the record online into EKIS. In EKIS, special software filters data records marked for SIS and communicates them to a special file in NSIS. Special software in NSIS further controls and communicates the data record to CSIS. However, data records under Articles 95 and 99 of the Convention, are first send by the special software program in EKIS to SIRENE, and SIRENE later communicates the records to CSIS. After the data records have been indexed at CSIS, they are redistributed to all Schengen Contracting Parties' NSISs, ready for search.

7.2.3 Access to Data

Access to data is required for various reasons: search, updating, correction, deletion, and individual access request (this will be discussed later as part of the external control). The objective of SIS is to offer online searchable access facilities for criminal and immigration authorities. Hence, search is the most common form of access to SIS. In data protection, the rule of thumb for access is necessity. The person who accesses the data must have a legitimate reason, such as fulfilling a public duty required of him/her. According to the findings from the interviews, access for purposes of search seems to be available to practically all officers responsible for border, crime, and immigration control in Austria. The number is not restricted and may increase as the need arises. The large number of people with access authority opens up the possibility for leakage of information.

Access for purposes of updating, correction and deletion of information is restricted and open only to DASTA officers who have the authority to enter data into SIS. Every six years, a control is made to ensure that the data are current. In normal cases, deletion of data happens automatically after the duration stipulated for storage expires (Article 112). The central system checks regularly for expiration dates. A month before deletion, a notice is automatically issued to the Contracting Party concerned and, unless they request retention, the data is automatically deleted.

In order to control access in general, a log audit is kept for all access to SIS. A log is created for every access. In the log audit, the user's identity or name, password, time, and reason for access are recorded. The Schengen Convention requires that every tenth query be recorded (Article 103). However, the practice in Austria is to log every query and the result. The log audits are stored at the EDP centre at the Ministry of the Interior and are deleted after six months, as required under the Convention.

To ensure data security, control of log audits is routinely performed. Currently, the control is done by use of a random generator send via emails to police divisions, requesting the reasons for access. Every week, 5 police divisions are controlled, involving a total of 20 persons. A project for control through online networks is on trial, and this will radically improve the number of controls. Where a violation of access rights is discovered, the officer concerned is reported to the criminal investigator, who may prosecute. So far, no reports on violations concerning SIS have been filed to the investigator. However, numerous violation reports have been filed concerning the national information system. As a result of a recent scandal concerning the national system, the Ministry of the Interior is considering to enhance access control and security by use of biometric options. Similar log audit procedures are kept for access to SIRENE.

SIS and SIRENE have separate networks for communicating information, encrypted to ensure security.

Although the access audits serve a useful role in monitoring use of the system, the DPC views the lack of manpower or capacity to control the log audits as critical. The data protection officer from the Ministry confirmed this. Currently, only about 20 persons in five police divisions are controlled every week. This is a very low number for a system that can be accessed by over 30,000 persons at any given time. As many protocols as possible should be controlled for the procedure to be effective.
In addition, the systems are most vulnerable to threats originating from within the system. Those authorised to access the system pose the biggest threat to the security of the system, as the recent scandal in Austria and earlier scandal in Belgium confirm. Although the Austrian incident did not involve SIS, it did, however, indicate that those who are entrusted with the system are its weakest link. Adequate control of log audits is important in order to forestall such scandals. Other measures, such as use of biometrics, would go a long way in relieving the problem. It is encouraging that the Ministry of the Interior is considering these possibilities as pointed out by the interviewees.

7.2.4 Organisational Controls

Organisational controls of a system involve personnel and procedures. As noted previously, SIS is an open-loop system, utilising people for its control function. Personnel are therefore a very important component of the internal control system. As discussed above, first level criminal officers are responsible for collection of data, and second level criminal officers for verifying and entering data into SIS. In addition, the Ministry of the Interior has appointed a person responsible for data protection and security in the national system. This person is also responsible for data protection and security in SIS. Furthermore, the responsibility for data protection in the police systems has been decentralised to each of the 9 police districts, each of which has a person responsible for data protection and security. The Ministry has also appointed a person responsible for security and data protection for SIRENE. This person is answerable to the overall data protection officer at the Ministry of the Interior. Procedures are regulations and technical control systems such as rules and procedures for deletion, updating, correction and access logs, as discussed above. However, a very important procedure not yet discussed is reporting. Reporting entails the making of documentation such as annual reports, educational material and other statistical material. This seemed completely absent in the Austrian SIS control systems. Such documentation is important for external control and transparency in the system (as discussed below).

7.3 External Control

External control refers to some form of institution or mechanism, independent of the system, such as supervision, audit, and parliamentary and judicial bodies. The importance of external control is not to replace internal control, which by all means is the most effective safeguard if it works properly, but to ensure that internal controls are working effectively. The Schengen Convention provides for two forms of external control: supervision (Articles 114 & 115), and judicial control. A third form of external control that may be added is individual right of access (Article 109). I regard the right of access as a form of external control, as it is not exercisable without the initiative of a data subject who is external to the system. I will now discuss these controls in relation to the findings from the interviews.

7.3.1 Supervision

The Schengen Convention provides for supervision at two levels: national (Article 114) and joint (Article 115). As regards *national supervision,* the Schengen Convention requires that each Contracting Party appoints a national authority to perform the task of supervising the national section of SIS, independently and in accordance with national law. In Austria, the DPC is such a body. It is independent and carries out controls and investigations on the national data systems and handles complaints from data subjects. According to findings from the interviews, the DPC has had occasion to carry out security controls on the national information system (NIS) and SIRENE but not NSIS. In 1998, it carried out a surprise control on SIRENE. The controls were targeted at persons with access authority and aimed at ensuring that they had the necessary knowledge and qualifications. Control has also been directed at technical security measures, such as logging audits to ensure that they are properly executed and controlled. However, as mentioned above, lack of personnel to control the log audits is a serious drawback.

As an appeal body for decisions made by the Ministry of the Interior, the DPC has not been very active because very few appeals relating to SIS have been made. So far, as far as I am aware, only one case has been appealed to the DPC and the decision of the Ministry was upheld. However, there have been many appeals relating to NIS.

Joint supervision of CSIS is allocated to the Joint Supervisory Authority (JSA). JSA must perform its tasks in accordance with the Schengen Convention, the Convention of the Council of Europe for the Protection of Individuals with regard to the Automatic Processing of Personal Data and the Recommendation of the Council of Europe regulating the use of personal data by the police, and pursuant to French law. However, the JSA lacks the necessary powers to make decisions and carry out investigations. Although it issues annual reports, it does not have the power to implement the recommendations. Furthermore, despite the new arrangement with the Council, providing the authority free access to carry out its work independently, the Council has control over the authority's budget. This may interfere with its independence. As it is presently constituted, the JSA may not be an effective external control.

7.3.2 Judicial Control

Judicial control, especially international or joint judicial control, was never a strong point in the Schengen co-operation. The Schengen Convention totally circumvented the idea of joint judicial control. However, the incorporation of the Schengen into the EU legal structure has acknowledged limited European Court of Justice jurisdiction. This may salvage the situation. Despite shortcomings in joint judicial control, national judicial apparatus of Contracting Parties remain the most viable judicial control organs regarding Schengen issues. In Austria, courts exercise judicial control as the appeal organs for decisions originating from the DPC. The DPC is the first level appeal organ concerning decisions of the Ministry of the Interior. It sits as a tribunal and reviews decisions made by the Ministry of the Interior. However, it has manifested little activity, as it has been rarely called upon to exercise its judicial review power. So far, it has done so in one case only. There have been practically no appeals against the decisions of the Ministry of the Interior. Whether this is an indication of the efficiency of the Ministry of the Interior in its internal control of SIS or in its decisions (as those from the Ministry were inclined to point out), or an indication of a lack of information on the part of data subjects on their rights, or due to the short time SIS has been operational, is difficult to tell. A combination of all these factors could be the explanation. In other jurisdictions: France, Germany, the Benelux, where SIS has been in operation for some time now, a significant number of cases are finding their way to the courts. In principle, an individual has a right of appeal, especially where one exercises the right of access, to the administrative Supreme Court, if not satisfied with the decision of the DPC. In addition, if the matter raises a constitutional question, a reference can be made to the Constitutional Court. Unlike the DPC, the courts have not had occasion to address a Schengen appeal case, as none has reached them yet.

Although joint judicial control was lacking in the earlier Schengen legal system, by extension of national judicial control, the European Court of Human Rights (ECHR) has joint control over appeals originating from Schengen Contracting Parties' courts. However, the ECHR may not yet have addressed such appeals. It takes a long time before individual applications meander through and exhaust national remedies. This could explain the present lack of such appeals to the ECHR. However, it is only a matter of time before appeals emerge, especially from the original Schengen Contracting Parties.

Judicial control is important especially in addressing wider questions of human rights and the interpretation of the Schengen Convention. Some national judicial decisions have pointed to the lack of clear registration and search criteria in the Schengen system, as practiced by the Contracting Parties. In France, in the case of a Romanian national, Mrs Forabosco, the court criticised the registration practice in Germany. Here, authorities register information about persons whose asylum application has been rejected. The French court asserted that such practice contradicts Article 96 of the Schengen Convention. In another French court decision, *Tribunal Administratif de paris v. Saïd* 1996, the court condemned French local authorities' search practise. A person from Algeria, with a valid residence permit in France, was issued a deportation order after reporting a change of residence address to the local authorities. The authorities searched SIS and found that the person had been registered as an unwanted person, to be refused entry under Article 96 of Schengen Convention by Belgian authorities, for an offence committed in Belgium while on a visit there. In its decision, the court held that the local authorities had no right of access to search SIS on basis of a report concerning change of residence address. These decisions also point to a need for joint judicial control in order to give a uniform interpretation of the provisions of the Convention, a responsibility the European Court of Justice should now have, despite its limited jurisdiction.

7.3.3 Individual Control

Under the Schengen Convention, where registration of data is required by law, and the individual has no right of consent or notification (where the data is recorded without the knowledge of the individual), exercise of individual control is dependent on the right of access. In theory, an individual has the power of control through exercising the right of access (Article 109 (1)), associated rights of correction or deletion (Article 110), and request of verification of data through national data protection authorities (Article 114). Obviously, the most important of these rights is the right of access. Without this, the exercise of the other rights may be rendered academic. Unfortunately, the right of access under the Schengen Convention is severely restricted. For example, where access requests fall under any of the exceptions (Article 109(2)), the practice in Austria is to inform the data subject that no data concerning her/him that can be communicated is registered. In Norway, a similar procedure has been adopted. Such ambiguity is found necessary in order not to reveal to the data subject that data concerning him/her is registered but cannot be revealed. However, in my opinion, this is unfortunate as the data subject is left in a state of limbo, not knowing whether any data about himself/herself is registered or not. This is especially the case where the data registered relates to ongoing criminal investigations or discreet surveillance. In such cases, an individual cannot exercise any control. In principle, if the individual is not satisfied with the reply, he/she may request the national data supervisory authority to check whether any data concerning himself/herself is registered. However, if the data falls under the above mentioned exceptions, the supervisory authority may not be allowed to reply to the data subject (Article 109(2)). In such circumstances, individual control may only be practical in cases where registered data does not fall under the exceptions and, given the nature of SIS, these may be very few indeed.

According to the findings of the interviews, the right of access is barely used in Austria. Although no long-term, concrete statistics were available, during the past four months (before March 2001), there had been about 1 200 requests concerning registration in SIS. According to my source of information, this is a high number of requests for such a short period. The upsurge of requests was attributed to a data registration scandal that had been publicised in the newspapers at the time, concerning the NIS, but not involving the SIS. The experience, as I was informed, was that whenever there was such a scandal, the rate of requests tended to increase and then fall and stabilise again. For example, during the nine month period prior to the scandal, the number of requests received was about 600. For most of these requests, there is no data registered in SIS. Requests for access are received from inside Austria, as well as from outside Austria and outside the Schengen area.

The right to have data corrected and deleted is practised in a similar manner as the right of access. If there is a need to correct or delete data, the request is normally complied with in cases where Austria is the reporting country. Where another Contracting Party has entered the data, the Ministry notifies the Contracting Party as soon as possible. The same procedure applies to updating data in SIS.

The exercise of individual control is also dependent on the information and knowledge available to the public in general about SIS. Unfortunately, the public seems to be poorly informed. This could partly explain the lack of enthusiasm in the exercise of the right of access exhibited by the general public. Lack of awareness on the part of the public can pose a serious threat to privacy and transparency of SIS, as individual's power to control is highly compromised. In Austria, except for the limited information given to the public during the launch of SIS in 1997, no other public information campaign has been carried out. As it transpired from the interviews, the Ministry of the Interior does not issue annual reports or any other documentation that could be of use to the public. The problem could be traced to the Schengen Convention, which imposes no requirement to inform the public. Even where such a requirement may be available under national law, it is unfortunately left to individuals to take the initiative. This is the case in Norway. The JSA has attempted to fill the informational gaps by placing brochures explaining individual's rights at airport terminals and other authorised crossing points at Schengen's external borders. It has also published alert statistics. However, they are not adequately informative, as they fail to specify the number of persons registered under each Article of the Schengen Convention.

8. Conclusion

In a system such as SIS, where individuals have restricted or no access of their personal information, only internal and external control mechanisms can ensure adequate individual protection. It is imperative, therefore, that those responsible for the system ensure proper internal control mechanisms. On the other hand, efficient external control should complement internal control in order to enhance overall individual protection. Both SIS internal control and external control mechanisms require fine tuning to ensure that innocent individuals do not become victims of the very system that is supposed to protect them. Areas of focus should be the collection and entry of data, control of access, public information and education, and both national and joint supervision. A requirement for a comprehensive data audit of all Schengen systems may be a viable solution for better and more comprehensive individual protection.

Notes and References