Articolo 19

Diritto di accesso

1. Chiunque desideri esercitare il suo diritto di accedere ai dati memorizzati presso l'Europol che lo riguardano o di fare verificare tali dati, può a tale scopo presentare a titolo gratuito una domanda, in uno Stato membro di sua scelta, all'autorità nazionale competente che la sottopone quindi senza indugio all'Europol e avvisa il richiedente che quest'ultimo gli risponderà direttamente.

2. ...

3. Il diritto della persona interessata di accedere ai dati che la riguardano o di farli verificare si esercita nel rispetto della legislazione dello Stato membro presso il quale essa l'ha fatto valere, tenendo conto delle disposizioni seguenti:

Qualora la legislazione dello Stato membro interpellato preveda la comunicazione relativa ai dati, quest'ultima è rifiutata se ciò è necessario:

1) per il corretto svolgimento delle funzioni dell'Europol,
2) per la protezione della sicurezza degli Stati membri e dell'ordine pubblico o per la lotta contro i crimini;
3) per la protezione dei diritti e delle libertà di terzi, e pertanto le esigenze delle persone interessate alla comunicazione devono passare in secondo piano.

4. ....

5. Il diritto alla verifica si esercita secondo le procedure seguenti:

Qualora la legislazione nazionale applicabile non preveda la comunicazione relativa ai dati o si tratti di una semplice domanda di verifica, l'Europol, in stretto coordinamento con le autorità nazionali interessate, procede alle verifiche e notifica al richiedente che le verifiche sono state effettuate, senza fornire indicazioni che possano rivelargli se abbia o meno informazioni sul suo conto.

La legge del Regno Unito sulla protezione dei dati, del 16 luglio 1998, contiene le seguenti disposizioni:

Parte II, Diritti dei soggetti titolari dei dati e di terzi

Sezione 7, paragrafo 1 - ..... chiunque ha diritto-

a) di essere informato dal responsabile del trattamento dei dati se i dati di carattere personale che lo riguardano sono oggetto di trattamento da parte o per conto del responsabile del trattamento dei dati; b) in tal caso, di ricevere dal responsabile del trattamento dei dati una descrizione i) dei dati di carattere personale cui egli ha diritto. c) di ricevere la comunicazione in formato intelligibile-i) le informazioni che rappresentano i dati di carattere personale che lo riguardano, …

Parte III, Esenzioni
Sezione 29, paragrafo 1- I dati di carattere personale trattati per una qualsiasi delle seguenti finalità
a) la prevenzione o l'investigazione di reati,
b) la cattura o il perseguimento giudiziario dei rei,
c) ...

sono esenti da ... e comunque dalla sezione 7, nella misura in cui l'applicazione ai dati di tali disposizioni potrebbe pregiudicare una qualsiasi delle materie menzionate nella presente sottosezione.

Parte V, Applicazione

Sezione 42, paragrafo 1

La persona che sia, o ritenga di essere, direttamente interessata dal trattamento di dati di carattere personale può avanzare una richiesta al garante, in proprio o per interposta persona, per valutare la probabilità o l'improbabilità che il trattamento sia avvenuto o avvenga in conformità con quanto disposto dalla presente Legge.

4) Qualora il garante abbia ricevuto una richiesta ai sensi della presente sezione egli notificherà alla persona che l'ha avanzata:
a) se ha proceduto ad una valutazione a seguito della richiesta e
b) nella misura in cui lo ritenga appropriato, tenuto conto in particolare di ogni eventuale esenzione di cui alla sezione 7 che si applichi in relazione ai dati di carattere personale di cui trattasi, le osservazioni formulate o le azioni intraprese a seguito della richiesta.

ARGOMENTAZIONI INNANZI IL COMITATO PER I RICORSI

Sig. X

Il ricorrente, ha ripetutamente affermato di essere oggetto di fastidi e discriminazioni da parte di vari individui quando si reca in Belgio e nei Paesi Bassi. Soltanto la polizia potrebbe aver orchestrato questi episodi e, se così fosse, sulla base di informazioni costruite e rilevate dall'Europol provenienti dal Regno Unito. La risposta fornita dall'Europol (la decisione del 22 gennaio 2001) alla sua richiesta (dell'8 gennaio 2001) nulla dice sul fatto che egli sia o meno noto all'Europol.

SNIC ed Europol

È desiderio della criminalità organizzata scoprire se le autorità sono al corrente delle loro attività, per cui essa investe risorse in vario modo per dare una risposta a questa domanda. Rivelare che nulla si sa sul conto di un individuo coinvolto nella criminalità organizzata è almeno importante quanto sapere che le organizzazioni preposte all'applicazione della legge sanno qualcosa. Se qualcuno che non ha collegamenti con la criminalità organizzata chiede di accedere a dati laddove non ci sono dati oggetto di trattamento, dicendo a tale persona che non ci sono dati che lo riguardano, si va a creare un precedente. Per precedente si intende il fatto che tale risposta dovrebbe essere fornita in tutte le circostanze simili in cui non si hanno dati a disposizione. Questo farebbe sì che un criminale inserito in un'organizzazione saprebbe che non ci sono dati che lo riguardano e con ciò ne trarrebbe un vantaggio. Fornire un vantaggio alla criminalità organizzata è contrario alle finalità dell'Europol e conseguentemente il precedente deve essere evitato. L'unico modo per evitarlo è dare una risposta alla richiesta di accesso come quella che è stata data.

CONCLUSIONI DEL COMITATO PER I RICORSI

Nella sua decisione del 13 dicembre 2001, in ragione delle speciali circostanze del caso, il comitato per i ricorsi aveva ritenuto appropriato che all'Europol venisse data l'opportunità di riesaminare la decisione. Il comitato per i ricorsi ha preso atto degli sviluppi successivi a tale decisione e pertanto limiterà le sue conclusioni alla decisione dell'Europol del 22 gennaio 2001.

In questo caso, il comitato per i ricorsi distingue due questioni.

La prima questione è la risposta data dall'Europol alla richiesta del sig. X di accedere ai dati che lo riguardano.

La Convenzione Europol, all'articolo 19, paragrafo 1, attribuisce il diritto di accesso a tutti gli individui. L'estensione di tale diritto non è specificatamente definita ma, alla luce

dell'articolo 14, paragrafo 1, della Convenzione Europol, deve essere considerata alla stregua del diritto definito dall'articolo 8 della Convenzione d'Europa del 28 gennaio 1981. Tale diritto consente ad ogni persona di accertare se sono stati archiviati dei dati di carattere personale che lo riguardano e, in caso affermativo, gli attribuisce il diritto di conoscerli. Il ricorso riguarda entrambi gli aspetti del diritto di accesso. Ai sensi dell'articolo 19, paragrafo 3, tale diritto va esercitato in conformità con la legislazione dello Stato membro in cui il diritto è invocato, in questo caso il Regno Unito. Questo articolo utilizza l'espressione — comunicazione relativa ai dati", che copre sia la comunicazione dell'esistenza di dati oggetto di trattamento, sia la comunicazione dei dati stessi oggetto di trattamento. Anche la legge sulla protezione dei dati del 1998 riconosce, alla sezione 7, paragrafo 1, il diritto di essere informati sul fatto che ci sono dati oggetto di trattamento ed insieme il diritto alla comunicazione di tali dati. L'esistenza di questi diritti nella legislazione dello Stato membro comporta l'applicabilità del secondo comma dell'articolo 19, paragrafo 3, il quale prevede strettamente i casi in cui la comunicazione vada rifiutata. Se una delle tre fattispecie di esenzione di cui all'articolo 19, paragrafo 3, è applicabile, la comunicazione deve essere rifiutata. Ciò significa che ogni richiesta di accesso in cui trovi applicazione il seconda comma dell'articolo 19, paragrafo 3, deve essere valutata caso per caso, per accertare la necessità di rifiutare la comunicazione in ragione di una delle fattispecie di esenzione. Per quanto l'esercizio del diritto di accesso debba avvenire in conformità con la legislazione dello Stato membro, è l'Europol che ha la responsabilità ultima di verificare l'applicabilità delle esenzioni di cui all'articolo 19, paragrafo 3.

La sezione 29, paragrafo 1, della legge sulla protezione dei dati del 1998 esclude dalla sezione 7 i dati di carattere personale trattati per la prevenzione o l'investigazione di reati e la cattura o il perseguimento giudiziario dei rei, quando l'applicazione della sezione 7 possa arrecare pregiudizio ad uno qualsiasi di questi elementi. Il contenuto di tali esenzioni è strettamente correlato all'esenzione di cui all'articolo 19, paragrafo 3, della Convenzione Europol.

Dalla seconda relazione presentata dal relatore risulta che la decisione dell'Europol è coerente con il parere, dato dall'Information Commissioner (garante delle informazioni) del Regno Unito ai responsabili del trattamento dei dati, circa la forma della risposta ad una richiesta di accesso dell'interessato quando non ci siano dati a disposizione o non ci si possa basare su un'esenzione.

Le argomentazioni utilizzate dall'Europol e dallo SNIC riguardano lo svolgimento delle mansioni dell'Europol, la protezione della sicurezza e dell'ordine pubblico, nonché la prevenzione del crimine, e sono strettamente correlate alla criminalità organizzata. Alla luce della legge e della prassi vigenti nel Regno Unito in merito al diritto di accesso ai dati riguardanti la criminalità organizzata nonché alla luce dell'articolo 19, paragrafo 3, della Convenzione Europol, la decisione dell'Europol rispetto alla richiesta del sig. X è conforme all'articolo 19, paragrafo 3, della Convenzione Europol.

La seconda questione riguarda la richiesta del sig. X di verificare i dati che lo riguardano. L'articolo 19, paragrafo 5, della Convenzione Europol si applica se la legge nazionale applicabile nulla dispone in merito alla comunicazione, oppure nell'ipotesi di una semplice domanda di verifica. Alla luce della sostanza di questo particolare ricorso, la domanda del ricorrente può essere vista come una semplice domanda di verifica. Questo significa che, ai sensi dell'articolo 19, paragrafo 5, della Convenzione Europol, l'Europol dovrà notificare al richiedente che sono state effettuate delle verifiche, senza però dargli alcuna informazione che gli possa rivelare se egli sia noto o meno.

SULLE SPESE

Poiché nessuna richiesta è stata fatta sulla base dell'articolo 27, paragrafo 1, del regolamento interno, non è necessaria alcuna decisione in merito alle spese.

DECISIONE

La decisione dell'Europol sulla richiesta avanzata dal sig. X di accedere ai dati che lo riguardano e di procedere alla loro verifica è conforme ai paragrafi 3 e 5 dell'articolo 19 della Convenzione Europol.

La presente decisione è resa nota in occasione della pubblica riunione del comitato per i ricorsi del 16 maggio 2002, trasmessa alle parti ed inoltrata all'autorità di controllo comune.

Bruxelles, 16 maggio 2002

Mario Manuel Varges Gomes
Presidente del Comitato per i ricorsi
dell'Autorità di controllo comune dell'Europol

F. MEMBRI

AUTORITÀ DI CONTROLLO COMUNE (ACC) DELL'EUROPOL
Presidente : Sig. Klaus KALK
Vicepresidente : Sig. Emilio ACED FELEZ

AUSTRIA

MEMBRI	*SUPPLENTI*
Sig.ra Waltraut KOTSCHY	Sig.ra. Birgit HROVAT-WESENER
Sig.ra Eva SOUHRADA-KIRCHMAYER	

BELGIO

MEMBRI	*SUPPLENTI*
Sig. Paul THOMAS	Sig. B. HAVELANGE
Sig. Bart DE SCHUTTER	

DANIMARCA

MEMBRI	*SUPPLENTI*
Sig.ra. Lena ANDERSEN	Sig. Peter AHLESON
Sig. Ib Alfred LARSEN	

FINLANDIA

MEMBRI	*SUPPLENTI*
Sig. Reijo AARNIO	Sig. Heikki HUHTINIEMI
Sig.ra Maija KLEEMOLA	

FRANCIA

MEMBRI	*SUPPLENTI*
Sig. Alex TÜRK	Sig.ra Marie GEORGES
Sig.ra Florence FOURETS	

GERMANIA

MEMBRI	*SUPPLENTI*
Sig. Joachim JACOB	Sig. Roland BACHMEIER
Sig. Klaus Rainer KALK	Sig.ra Birgitte SCHERBER-SCHMIDT

GRECIA

MEMBRI	*SUPPLENTI*
Sig. Sotirios LYTRAS	Sig. Georgios DELIGIANNIS
Sig.ra Koustoula KAMBOURAKI	

IRLANDA

MEMBRI	*SUPPLENTI*
Sig. Joseph MEADE	Sig. Tom MAGUIRE

ITALIA

MEMBRI	*SUPPLENTI*
Sig.ra Vanna PALUMBO	
Sig. Giuseppe BUSIA	

LUSSEMBURGO

MEMBRI	*SUPPLENTI*
Sig. Georges WIVENES	Sig. Pierre WEIMERSKIRCH
Sig. Edouard DELOSCH	

PAESI BASSI

MEMBRI	*SUPPLENTI*
Sig. Peter J. HUSTINX	Sig.ra Evelien van BEEK
Sig. Ulco van de POL	

PORTOGALLO

MEMBRI	*SUPPLENTI*
Sig. Mário Manuel VARGES GOMES	Sig.ra Isabel CERQUEIRA DA CRUZ
Sig. Amadeu Francisco RIBEIRO GUERRA	

SPAGNA

MEMBRI	*SUPPLENTI*
Sig. José Luis PIÑAR MAÑAS	Sig.ra Concepción ROMERO CIQUE
Sig. Emilio ACED FELEZ	Sig.ra Mercedes ORTUNO

SVEZIA

MEMBRI	*SUPPLENTI*
Sig. Ulf WIDEBÄCK	Sig.ra Agneta RUNMARKER
Sig. Leif LINDGREN	Sig.ra Britt-Marie WESTER

REGNO UNITO

MEMBRI	*SUPPLENTI*
Sig. Richard THOMAS	Sig. David SMITH
Sig.ra Francis ALDHOUSE	

COMITATO PER I RICORSI DELL'ACC

Presidente:	Sig. Mário Manuel VARGES GOMES
Vicepresidente :	Sig. Ulf WIDEBÄCK

AUSTRIA

MEMBRO	*SUPPLENTE*
Sig.ra Waltraut Kotschy	Sig.ra Birgit Hrovat-Wesener

BELGIO

MEMBRO	*SUPPLENTE*
Sig. Paul Thomas	Sig. Bart de Schutter

DANIMARCA	
MEMBRO	*SUPPLENTE*
Sig.ra Lena Andersenensen	Sig. Peter Ahleson
FINLANDIA	
MEMBRO	*SUPPLENTE*
Sig. Reijo Aarnio	Sig.ra Maija Kleemola
FRANCIA	
MEMBRO	*SUPPLENTE*
Sig. Alex Türk	Sig.ra Florence Fourets
GERMANIA	
MEMBRO	*SUPPLENTE*
Sig. Joachim Jacob	Sig. Roland Bachmeier
GRECIA	
MEMBRO	*SUPPLENTE*
Sig. Sotirios Lytras	Sig.ra Koustoula Kambouraki
IRLANDA	
MEMBRO	*SUPPLENTE*
Sig. Joseph Meade	Sig. Tom Maguire
ITALIA	
MEMBRO	*SUPPLENTE*
Sig. Giuseppe Busia	Sig.ra Vanna Palumbo
LUSSEMBURGO	
MEMBRO	*SUPPLENTE*
Sig. Georges Wivenes	Sig. Edouard Delosch
PAESI BASSI	
MEMBRO	*SUPPLENTE*
Sig. Peter .J. Hustinx	Sig. Ulco. van de Pol
PORTOGALLO	
MEMBRO	*SUPPLENTE*
Sig. Mário Manuel Varges Gomes	Sig.ra Isabel Cerqueira da Cruz
SPAGNA	
MEMBRO	*SUPPLENTE*
Sig. Emilio Aced Felez	Sig.ra Concepcion Romero Cique
SVEZIA	
MEMBRO	*SUPPLENTE*
Sig. Ulf Widebäck	Sig. Leif Lindgren
REGNO UNITO	
MEMBRO	*SUPPLENTE*
Sig. Francis Aldhouse	Sig. David Smith

XII - Autorità comune di controllo Schengen

79 Sixth report january 2002 - december 2003 Activities of the Joint Supervisory Authority

Foreword

Eight years have elapsed since the Schengen Information System (SIS) was set up, and now the Joint Supervisory Authority (JSA) in Brussels is submitting its sixth Report.

This document sums up the activity carried out by the JSA in the past two years. Like other texts of this kind, it contains references to initiatives, information campaigns for citizens, decisions, institutional relationships and results achieved, without dwelling on the details – which can be found in the documents adopted by the JSA as well as on its new web site.

Still, this Report has a special value in that it is published on the eve of an historical event – namely, setting out the activities required to deploy, by 2006, a second-generation Information System, called SIS II, which will bring about major innovations and impact considerably on vital functions for Europe and its citizens' rights and fundamental freedoms.

The JSA intends to play a leading role in this major change process by contributing to its guidance.

The SIS is already the largest European centralised database within the framework of the initiatives concerning visas, immigration, and police and judicial cooperation.

Other short-term proposals to amend the Schengen Convention are at an advanced stage of discussion.

As for the long term, the JHA Council of 5-6 June 2003 decided that several new categories of alert, new research fields, interlinks, new purposes, new sensitive categories of personal data – such as biometric data –, new retention periods, and new, larger categories of system user would have to be taken into account for the SIS II.

The purposes to be achieved in future are also important for our democratic societies, however it is necessary to assess their proportionality and carry out a prior checking exercise with regard to the impact that these will have on the rights and fundamental freedoms of the millions of individuals that will be involved for diverse reasons.

The envisaged high-level security measures are not enough. The SIS II should not merely represent a second-generation system from a technical point of view. A revised set of data protection provisions is also required. These should be easy to understand and better known to individuals and practitioners as well as being equal to the challenges posed by the SIS II, providing adequate safeguards and ensuring that the system is consistent with its own purposes.

Data protection does not entail deciding whether given information is to be disclosed or not. In fact, it consists in a more pervasive exercise aimed at affording safeguards, balancing interests, devising proportionate solutions, and organising information flows.

It is necessary to create the best mix between effective police and judicial cooperation and the fundamental right to personal data protection, which has been enshrined in the Charter of Fundamental Rights of the European Union.

The continuing harmonisation of databases in the so-called First and Third Pillars is expected. We call on the other institutions to develop a clear-cut privacy policy as well as a clear-cut concept of the new forms of cooperation that are to replace the compensatory measures originally laid down in the Schengen Convention.

Schengen, Europol, Eurodac, the Visa Information System (VIS) and other systems were set up in different manners, in different periods and for different purposes. Now is the time to enhance the safeguards against the risks of gaps and overlapping, reduce uncertainties further, and do away with merely formal safeguards, lack of information, and sluggish cooperation.

This is why the JSA is grateful to the other institutions, and in particular to the European Parliament, for their closer collaboration, which was fruitfully enhanced in the past few months – in particular with regard to the Spanish proposals to amend the Schengen Convention, the Recommendation adopted by Parliament on 20 November 2003, and the ad hoc workshop held in Brussels on 6 October.

At the latter workshop, the JSA drew the participants' attention to five main requirements:

1) Ensuring that the initiatives concerning the SIS II are reconciled with all the other institutional activities already in progress, such as the Spanish proposals on SIS I, the amendments to the Schengen Convention with regard to trafficking in stolen vehicles, implementing the European arrest warrant, the VIS, and the Greek initiative on the procedure to amend the SIRENE Manual, also with a view to sensible, cost-effective expenditure,

2) Ensuring that the provision for a timely data protection assessment is included in the initial layout of the contract to be granted in 2004 with regard to the SIS II following the public call for tenders,

3) Ensuring effective, continued cooperation with the JSA as shown by the constructive relationship that was developed of late between the JSA and the European Commission,

4) Setting out the objectives of the SIS II prior to laying down its technical features so as to ensure that the new system can work in a logical fashion from the start, and

5) Encouraging improved quality in data protection aimed at more substantive safeguards, by ensuring that the system and its intelligent functions can really be monitored, that it is highly transparent for citizens, and that no redundant data and/or databases are present.

This is a time of strategic importance for the European Union, and data protection is bound to play a specific role.

The SIS II will only manage to be a success story if it is really data protection-oriented. For its part, the JSA is aware that it is entitled to play the enhanced role called for by the European Parliament as well as be provided with a specific budget and adequate resources. The JSA shall also actively cooperate with the European Data Protection Supervisor, and it will continue its activity to address the important issues coming up in the next two years.

The Schengen Joint Supervisory Authority

SCHENGEN JSA ACTIVITY REPORT

CHAPTER 1

1.1. Schengen: the Background

1.1.1. Introduction

Enshrined in the Treaty of Amsterdam, which came into effect in 1999, is the concept of a European Union in which the free movement of persons is assured.

The first steps towards creating an area of free movement came with the Schengen Agreement, signed by France, Germany and the Benelux countries in 1985. Implementing the Agreement, the Schengen Convention of 1990 abolished the internal borders of the signatory states and created a Schengen area with a single external frontier where immigration checks were to be carried out in accordance with a single set of rules.

In response to fears that the unchecked movement of goods and people would be open to abuse, the Convention contained a number of compensatory measures. These included measures to facilitate closer co-operation between border authorities, and the creation of the Schengen Information System (SIS).

1.1.2. The Schengen Information System (SIS)

The SIS is an information system linking up all the states applying the Schengen Convention and the competent authorities in each of those states. National police, customs and border control authorities in the Schengen States use the SIS to make police and customs checks on persons and objects by means of an automatic search procedure. Checks are also made by immigration officials when processing persons from non-Schengen States.

The Schengen Convention specifies the categories of information that may be held in the SIS. National authorities may enter information on certain objects, such as stolen vehicles, and on the following categories of person:

1. persons wanted for arrest for extradition purposes
2. persons refused entry to the Schengen area
3. missing persons or persons who need to be placed under protection
4. persons sought by judicial authorities in connection with criminal proceedings
5. persons who are to be the subject of discreet surveillance or a specific check

The SIS is made up of national sections (NSIS), which can be checked by the authorities competent for making border, customs and police checks; and a central section (CSIS) located in Strasbourg. The authorities in a particular state can search only their own NSIS data file, and each national authority has access to those categories of data needed to carry out its specific checks. Immigration authorities, for example, may only access information concerning persons refused entry to the Schengen area.

To enter information into the system, national officials must first send the information to the national authority responsible for their national section of the SIS (these authorities are known as the SIRENE bureaus). The national SIRENE bureau has to ensure that the information is relevant to the SIS and that Schengen rules have been applied correctly. If so, the information is forwarded to the central section of the SIS, which then updates each national section with the new entry. This ensures that each national section of the SIS is identical to the central section.

1.1.3. The Joint Supervisory Authority

It is important for a complex Europe-wide information system of this kind to adhere to the principles of data protection. Given that a person may be refused access to the Schengen area on the basis of information held in the SIS, it is obviously essential that such information should be accurate and up-to-date, for example.

As a safeguard, the Convention contains a number of provisions relating to data protection; it also established an independent authority – the Joint Supervisory Authority (JSA) – charged with inspecting the central section of the SIS, examining any difficulties of application or interpretation that may arise during the operation of the SIS, and ensuring that the SIS complies with the various data protection provisions mentioned in the Schengen Convention. The JSA comprises two representatives from the national data protection authority of each Schengen State.

1.1.4. Incorporating Schengen into the European Union

Although Schengen began as an intergovernmental convention, the Schengen Convention and the various decisions adopted under it – known collectively as the Schengen acquis – were integrated into the legal and institutional framework of the European Union by the Treaty of Amsterdam. The JSA views this as a positive move, opening Schengen to transparent parliamentary and judicial scrutiny.

The Schengen Agreement paved the way for the area of freedom, justice and security envisaged in the Treaty of Amsterdam. It has since been declared that this area 'should be based on the principles of transparency and democratic control' [1], and it is in this context that the JSA seeks to carry out its tasks. This activity report provides an overview of these tasks, summarising the activities undertaken and the opinions issued over the past two years.

1.2. The Changing Face of the Schengen Information System: SIS II and Other Developments

1.2.1. SIS II

Now, eight years after the introduction of the SIS, the process of replacing the system is under way. There are various reasons for this. The enlargement of the European Union brings with it the need to develop a new system capable of processing a huge amount of information; in addition, those with practical experience of the SIS have been suggesting ways in which the system might be improved. At the same time, developments in the ongoing fight against crime and terrorism, including the creation of new institutions such as Europol and Eurojust, have led to calls for the information held in the SIS to be used for a wider purpose. A new system, SIS II, is being developed and is scheduled to come into operation in 2006.

1.2.2. Initiatives to Amend the Schengen Convention

There are several initiatives to change the SIS even before this new system comes into being. Foremost among these is a Spanish initiative (2) which, among other things, is intended to allow Europol and Eurojust to access the SIS. Another initiative concerns the proposed introduction of a European arrest warrant, which is likely to result in additional categories of information being held in the the SIS.

There are, essentially, two trends that are of particular concern to the JSA. The first relates to the information held in the SIS, with moves to add new categories of information and introduce new types of information, such as biometric data. The second trend concerns access to and use of data held in the SIS. There are proposals to allow other organisations to access the SIS – Europol and Eurojust have already been mentioned – and this is a trend

(1) Taken from the general conclusions of the European Council convened in Tampere in 1999
(2) Official Journal C160, 04/07/2002

that looks set to continue. As this happens, it becomes increasingly likely that data held in the SIS will be used for a wider range of purposes.

The JSA recognises that the SIS has proved to be an essential instrument for safeguarding security across the Schengen area; while at the same time, the rights of individuals whose information is processed in the SIS have been protected by an adequate system of data protection rules and measures.

1.2.3. The Joint Supervisory Authority's Approach

The JSA has warned that, as they stand, these proposals would result in a fundamental change to the nature of the system: whereas the SIS simply alerts the relevant authorities that a particular person is wanted for one of the reasons laid down in the Schengen Convention, the SIS II looks set to become a multi-purpose investigation tool.

As the EU is faced with the prospect of a new system that would allow authorities to share information on millions of individuals for a variety of purposes – possibly using the latest technologies to process sensitive biometric data – there is a clear need for careful consideration of the impact this may have on the rights of individuals. It is necessary to examine all proposals for the SIS II in order to ensure respect for fundamental human rights, and in particular the right to personal data protection that was recently re-affirmed by Article 8 of the Charter of Fundamental Rights of the EU.

In dealing with these various developments, the JSA has set out to:

- raise awareness of any proposals to change the Schengen Convention or the SIS;
- encourage parliamentary scrutiny of such proposals; and
- forge close working relationships with the institutions involved in developing policy on Schengen – particularly the European Parliament, the Council and the European Commission – in order to ensure that the highest standards of data protection are built into the new system.

During the course of 2002 the JSA issued three opinions on the proposals to introduce new functions to the SIS. In these opinions the JSA expressed concern about the moves to allow organisations such as Europol access to the SIS, and requested a more thorough examination of the implications of storing biometric data in the SIS. These opinions are addressed in more detail in the second Part of this report.

The JSA has made efforts to bring the debate on changing the SIS to the fore. On 6 October 2003, a hearing on SIS II was held at the European Parliament before the Committee on Citizens' Freedoms and Rights, Justice and Home Affairs. The hearing provided an opportunity for the JSA to make its position clear. The JSA's chairman, Mr Buttarelli, made a presentation in which he stressed that the SIS II would not be effective if it failed to adhere to data protection principles. He added, however, that data protection need not be an obstacle to change, and that the JSA would be willing to play a constructive role in the development of a second generation SIS. As well as presentations from a number of experts in the field of data protection, the hearing also heard from those with direct responsibility for developing the SIS II, such as Commissioner Vitorino. The JSA was encouraged to note that there was considerable interest from Members of the European Parliament, particularly with regard to the implications of the resulting system on the rights of individuals.

The JSA has sought to co-operate with all bodies involved in the development of the SIS II, both at European level and at national level, and it has urged these bodies to work together to ensure that the highest standards of data protection are built into the new system.

The chairman of the JSA attended another hearing before the Committee on Citizens' Freedoms on 25 March 2003. Entitled 'Data Protection since 11 September 2001: What

Strategy for Europe?', the hearing examined recent developments and the potential implications for data protection. This hearing, together with the hearing in October, helped to build on the JSA's links with the European Parliament, and the Committee on Citizens' Freedoms in particular.

The JSA has been in close dialogue with the Article 36 Committee (the Committee responsible for preparing the ground for Council deliberations on police and judicial co-operation). In a meeting between the chairman of the JSA and the chairman of the Article 36 Committee in February 2002, it was agreed that the Article 36 Committee would forward all relevant documents to the JSA as quickly as possible.

In addition, the JSA has been developing links with the European Commission. The Commission, which is responsible for funding and developing the SIS II, recently sent the JSA a copy of a feasibility study, covering technical and organisational aspects of the development and installation of the new system. Officials from the Commission's IT unit attended the JSA's meeting in December 2003, and provided an overview of the developments that have taken place so far. The Commission representatives have agreed to attend the next meeting of the JSA in 2004, and this will provide the JSA with the opportunity to pose questions on specific aspects of the development process.

CHAPTER 2

2.1. THE WORK OF THE JOINT SUPERVISORY AUTHORITY

2.1.1. How the JSA Operates

The JSA comprises delegations from the 15 countries with information currently in the SIS: namely, Austria, Belgium, Denmark, Finland, France, Germany, Greece, Iceland, Italy, Luxembourg, the Netherlands, Norway, Portugal, Spain and Sweden. Each of these countries may have two members and two alternate members. Ireland and the UK, together with the ten countries that are soon to join the EU, have been granted observer status.

The JSA usually meets quarterly, though there is the possibility of holding extraordinary meetings to discuss issues requiring immediate attention. On 7 October 2003, for example, the JSA met to discuss the hearing on SIS II that had been held in the European Parliament the previous day. Over the course of the last two years the JSA has convened ten meetings.

The members of the JSA elect a chairman and a vice-chairman to preside over meetings. According to the JSA's rules of procedure each can serve for up to two one-year periods. In December 2003 Mr Buttarelli completed his second term of office. The vice-chairman, Mr van de Pol, was elected chairman at the JSA's meeting of 11 December 2003. At the same meeting Ms Cruz was elected as the new vice-chairman.

Although the JSA strives to reach decisions by consensus, in cases where this is not possible members may decide to hold a vote, with each delegation entitled to a single vote. Those delegations with observer status do not have voting rights.

2.1.2. Working Together: Data Protection and the Europe-Wide Information Systems

Moves to facilitate co-operation between police and judicial authorities of the EU Member States have led to the creation of other Europe-wide information systems. Apart from the SIS, the two main systems operating in this field are the Europol information system and the Customs Information System.

Each system has an independent joint supervisory authority charged with ensuring that

the systems comply with data protection provisions. These two joint supervisory authorities share some similarities with the Schengen JSA: all three authorities are made up of representatives from the national data protection authorities, they are all served by the same joint secretariat based in Brussels, [3] and they deal with many issues of a similar nature. With this in mind there have been recent attempts to co-ordinate the efforts of the different authorities.

- In March 2003 the three joint supervisory authorities set up a working group to review, from a data protection perspective, the existing Europe-wide information systems. This working group was given a mandate to examine the existing systems in order to ascertain whether the purposes of the different systems overlap, and to consider the implications of future developments.

- The three authorities also established a technical group. Consisting of technical experts from the data protection authorities of the various Member States, this group provides technical support to the joint supervisory authorities. The group is currently in the process of developing a standard tool for inspecting the three information systems.

As a footnote, it is worth mentioning the role of the European Data Protection Supervisor. [4] The Supervisor, who has yet to be appointed, will be responsible for monitoring that information in the SIS which relates to immigration (specifically, alerts entered under Article 96). For this reason it will obviously be important to ensure that the Schengen JSA works with the Supervisor to develop a co-ordinated approach to supervising the SIS.

2.2. ACTIVITIES

2.2.1. Raising Awareness

The JSA aims to ensure that individuals are informed of the rights they have under the Schengen Convention.

Briefly, these rights are:

1. the right of access to information held on you in the SIS
2. the right to correct such information if it is factually incorrect or to have it deleted if it is held unlawfully
3. the right to bring an action to correct, delete or obtain information, or to obtain compensation
4. the right to ask a national data protection authority to check the information held on you in the SIS

The JSA's first information campaign in 1998 resulted in the publication of a rights leaflet. The distribution of this leaflet, which informed individuals of the rights they have in relation to information held on them in the SIS, led to a significant increase in the number of requests for access. The JSA has decided to publish a new edition of the rights leaflet and this will soon be available at airports and other national entry points throughout the Schengen area.

Individuals can exercise their right of access in any of the states in the Schengen area, but the procedure varies depending on the national law of the state in which access is requested. In 2002, the JSA produced a booklet – The Guide – which provides details of the procedure to be followed in each of the Schengen States. This information can now be found on the JSA's web site.

In July 2003 the JSA launched a new web site with the intention of providing easy access to the opinions and recommendations of the JSA. The site, which will be maintained by the secretariat, is currently available in English but work is under way to make it available in all

EU languages. The web site address is www.schengen-jsa.dataprotection.org.

In October 2003 the JSA issued its first newsletter. The newsletter was produced in time for the hearing on SIS II at the European Parliament and it contained information on the ongoing work of the JSA. The JSA intends to publish such a newsletter – or perhaps a news update on the web site – on a regular basis.

As well as ensuring that individuals are informed of their rights, the measures outlined above, and the development of the web site and the newsletter in particular, are also intended to raise the profile of the JSA. It is important that other bodies have the opportunity to see exactly what the JSA does. Moreover, increasing awareness of the JSA among the key decision-making bodies of the EU will enable the JSA to voice its concerns with more effect. In addition, such bodies might feel more inclined to consult the JSA to ensure that data protection considerations are taken into account.

2.2.2. Inspection

The JSA has the task of ensuring that the technical support function of the SIS (the CSIS) complies with the data protection principles set out in the Schengen Convention and the other legal texts on data protection mentioned in that Convention, such as the Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data of 28 January 1981.

In December 2002, the JSA set up an inspection team to inspect the CSIS for the second time. The inspection team visited the CSIS in Strasbourg on 25 and 26 March 2003.

The inspection team developed provisional checklists setting out the checks to be carried out during the in situ inspection. These checks covered documents, systems, the procedures applied and the people involved in the processing of data.

Since the JSA's last inspection report (adopted on 1 November 1999) the support function of the SIS has been modified. The JSA considers the present system, known as CSIS1+, to be an improvement on the previous system in so far as compliance with the relevant data protection principles is concerned.

The general conclusion was a positive one. The JSA did, however, adopt some recommendations – largely technical in nature – in order to further improve compliance with the Convention and other related data protection provisions. The latest inspection report was adopted by the JSA at its meeting on 25 September 2003 and it was agreed that the inspection team should monitor the extent to which its recommendations have been followed in March 2004, six months after the adoption of the report.

It is worth noting that during the course of this inspection the team had the full co-operation of the staff responsible for managing the CSIS.

2.2.3. Third Country Nationals and Access to the Schengen Area – Article 96 Data

Under Article 96 of the Schengen Convention, the authorities in Schengen States may enter alerts on third country nationals refused entry to the Schengen area. Article 96 stipulates that before such an alert can be entered there must first have been a national alert resulting from a decision taken by the competent administrative authorities or courts in accordance with the rules of procedure laid down by national law.

The vast majority of alerts on persons held in the SIS have been entered under Article 96, and the JSA has decided to focus on the issue of Article 96 and on the way in which it is applied in the different Schengen States.

An action plan was drawn up and it was agreed that each national data protection authority should check whether personal data entered by the authorities in their country

had been entered in compliance with the provisions of Article 96. It was also decided that the JSA should look to assess, in the short term, the application and interpretation of Article 96 in the different countries of the Schengen area.

The JSA first set out to produce an overview of the various national laws that lead to a decision resulting in an Article 96 alert. To this end, a questionnaire was drawn up and sent to the national data protection authorities of the Schengen States. Results are now being compiled. The JSA's next step has been to develop a methodology for examining Article 96 alerts and the extent to which they comply with the relevant national regulations.

The results from the investigation into the use of Article 96 will require complex analysis, and the whole process is expected to continue for the next two years.

2.3. OPINIONS

2.3.1. Changes to the SIS

2.3.1.1. Spanish Initiative and Other Proposals to Change the SIS

The JSA has issued three opinions on the proposals to change the Schengen Convention: in June, October and December 2002.

The JSA noted that the proposals to grant Europol and Eurojust access to the SIS amounted to a fundamental departure from the basic principles of Article 102 of the Schengen Convention, which limits the use of Schengen data to the purposes laid down in each category of alert. Furthermore, the JSA stressed that the tasks for which these organisations might access the SIS must be in compliance with those articles of the Schengen Convention that deal with access to and use of SIS data. There is need for clarification of the specific tasks for which Europol and Eurojust will require access to SIS data. In general, the JSA is of the view that more information on these proposals is needed.

Proposals to include biometric data in the SIS are of concern to the JSA. Once again, the JSA stated in its opinions that it needed more information in order to make a proper assessment of the implications. There would appear to be two developments: first is the proposal to introduce fingerprints and photographs and, second, the suggestion that the SIS might process other, more sensitive biometric data in the future. It is argued that it is necessary for the SIS to hold fingerprints and photographs so as to identify a particular individual when there are doubts concerning identity. However, the JSA remains of the view that photographs and fingerprints should only be incorporated where it is essential for the execution of an alert and, to date, the JSA has not been presented with any information to suggest that it is necessary to process such information in the case of all alerts. Moreover, a number of questions remain. Will this information only be accessible after a hit and when needed for identification? What conditions will be in place to safeguard the rights of individuals? In any case, there ought to be a full and open discussion of the implications of creating a Europe-wide information system in which sensitive biometric data – such as DNA data – are processed.

2.3.1.2. The European Arrest Warrant

A Framework Decision has been drawn up with a view to replacing the existing extradition arrangements with a European arrest warrant. The European arrest warrant is defined as any judicial decision issued by a Member State with a view to the arrest or surrender by another Member State of a requested person. This may be done for the purposes of conducting a criminal prosecution, for example. Listed in a specimen form attached to the Framework Decision are certain categories of information which the European arrest warrant must contain: these include information on the identity of the person concerned, the issuing judicial authority and the nature of the offence. If this additional information were

to be communicated via the SIS, the SIS would have to be altered considerably.

Although the JSA has not yet issued an opinion on this topic, it has asked the Article 36 Committee whether the categories of information set out in the specimen form attached to the Framework Decision will be incorporated into the SIS. The Article 36 Committee has since confirmed that this is the intention.

2.3.1.3. Accession of Ireland and the UK

In 1999 the UK asked to take part in some aspects of Schengen: namely, co-operation in criminal matters, the fight against drugs, and the SIS. The UK request was approved by Council Decision in May 2000. Ireland asked to participate in some aspects of Schengen in 2000, and in all the provisions concerning the implementation and operation of the SIS. In February 2002 the Council adopted a Decision approving Ireland's request.

Both countries are required to comply with the data protection provisions set out in the Schengen Convention in those areas where they apply the Schengen acquis. In order to assess the level of data protection in both countries the JSA asked the Irish Data Protection Commissioner and the UK's Information Commissioner – who have both been granted observer status by the JSA – to provide documents detailing their national data protection legislation. They were also asked to indicate whether they would take account of the JSA's opinions. Both Commissioners submitted the requested information and, after evaluating the documents, the JSA concluded that from a data protection perspective there were no objections to the accession.

2.3.1.4. Implementation of Schengen in the UK

The UK opted to participate in the provisions of the Schengen acquis concerning the establishment and operation of the SIS except in respect of those provisions concerning alerts entered, for immigration purposes, on persons to be refused entry to the Schengen area (Article 96 alerts).

In 2001 the UK submitted a proposal for implementing the SIS in the UK. However, the JSA voiced concerns about this proposal, as it would lead to the processing of Article 96 data in the UK. This would be in breach of Article 94 of the Schengen Convention which expressly limits the processing of data in the NSIS to those data required for the purposes laid down in the Schengen Convention. In other words, given that the UK would not be applying Article 96 of the Convention, Article 96 data should not be processed in the UK.

The JSA did accept, however, that the UK would need limited access to Article 96 alerts in order to comply with Article 107 of the Convention which requires the state entering an alert to ascertain whether the person on whom the alert is being entered is already the subject of an alert in the system.

In an attempt to allay these concerns the UK gave assurances that although all SIS data would be sent to the UK, Article 96 data would be filtered out at the UK NSIS. This filtered database would be the only one to which all end users would have access – with access to Article 96 data restricted to a limited number of staff. In an opinion issued in February 2002, the JSA made it clear that any mechanism in which Article 96 data were sent to the UK would be in breach of Article 94 and, as such, unacceptable.

A solution was found with the proposal that a filter should be placed at the CSIS in Strasbourg. This filter will prevent Article 96 data from being transmitted to the UK in the first place. New UK alerts will be checked against the existing Article 96 alerts at the CSIS and an automated message will then be sent to the UK in cases where a double alert is found; if further investigations reveal that the alerts do not concern the same person, the UK alert will be accepted by the CSIS and sent out as any other alert.