EUROPEAN DATA PROTECTION SUPERVISOR

Opinion of the European Data Protection Supervisor

— on the Proposal for a Council Decision on the establishment, operation and use of the Second Generation Schengen Information System (SIS II) (COM(2005)230 final);

— the Proposal for a Regulation of the European Parliament and of the Council on the establishment, operation and use of the Second Generation Schengen Information System (SIS II) (COM(2005)236 final), and

— the Proposal for a Regulation of the European Parliament and of the Council regarding access to the Second Generation Schengen Information System (SIS II) by the services in the Member States responsible for issuing vehicle registration certificates (COM(2005)237 final)

(2006/C 91/11)

THE EUROPEAN DATA PROTECTION SUPERVISOR,

Having regard to the Treaty establishing the European Community, and in particular its Article 286,

Having regard to the Charter of Fundamental Rights of the European Union, and in particular its Article 8,

Having regard to Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data,

Having regard to Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data, and in particular its Article 41,

Having regard to the request for an opinion in accordance with Article 28 (2) of Regulation (EC) No 45/2001 received on 17 June 2005 from the Commission;

HAS ADOPTED THE FOLLOWING OPINION:

1. INTRODUCTION

1.1. Background

The Schengen information system (the SIS) is an EU large scale IT system created as a compensatory measure following the abolition of controls at internal borders within the Schengen area. The SIS allows competent authorities in Member States to exchange information which is used for performing controls on persons and objects at the external borders or on the territory, as well as for the issuance of visas and residence permits.

The Schengen Convention entered into force in 1995, as an intergovernmental agreement. The SIS, as part of the Schengen Convention, was later on integrated into the EU framework by the Amsterdam Treaty.

A new 'second generation' Schengen Information System II will replace the current system, so allowing the enlargement of the Schengen area to the new EU Member States. It will also introduce new functionalities in the system. The Schengen provisions elaborated in an intergovernmental framework will be fully transformed in classic European law instruments.

On 1 June 2005, the European Commission presented three proposals for establishing the SIS II. These proposals consist of:

— a proposed Regulation based on Title IV EC Treaty (visas, asylum immigration and other policies related to the free movement of persons) which will govern the first pillar (immigration) aspects of the SIS II, hereinafter referred to as 'the proposed Regulation';

— a proposed Decision based on Title VI EU Treaty (police and judicial cooperation in criminal matters) which will govern the use of SIS for third pillar purposes, further referred to as 'the proposed Decision';

— a proposed Regulation based on Title V (Transport) regarding specifically the access to the SIS data by authorities in charge of vehicle registration; this proposal will be addressed separately (see below, point 4.6).

It is worth mentioning in this context that the Commission will issue in the coming months a communication on interoperability and increased synergies between EU information Systems (SIS, VIS, Eurodac).

The SIS II consists of a central database called the 'Central Schengen Information System' (CS-SIS) for which the Commission will ensure the operational management connected to national access points defined by each Member State (NI-SIS). SIRENE authorities shall ensure the exchange of all supplementary information (information connected to the SIS II alerts but not stored in the SIS II).

Members States will contribute data to the SIS II on people wanted for arrest, surrender or extradition, people wanted for judicial procedures, people to be placed under surveillance or subject to specific checks, people to be refused entry at external border and lost or stolen items. A set of data called 'alerts' entered in the SIS allows the competent authority to identify a person or an object.

The SIS II develops new characteristics: widened access to the SIS (Europol, Eurojust, national prosecutors, vehicle licensing authorities), interlinking of alerts, addition of new categories of data, including biometric data (fingerprints and photographs), as well as a technical platform to be shared with the Visa Information System. These additions have stirred discussions for years about a shift of purpose of the SIS, from a control tool to a reporting and investigation system.

1.2. **General assessment of the proposals**

1. The EDPS welcomes the fact that he is consulted on the basis of Article 28 (2) of Regulation (EC) No 45/2001. However, in view of the mandatory character of Article 28 (2), the present opinion should be mentioned in the preamble of the texts.

2. For several reasons, the EDPS welcomes the proposals. The transformation of an intergovernmental structure into European law instruments brings several positive consequences: the legal value of the rules governing SIS II will be clarified, the Court of Justice will have competence for the interpretation of the first pillar legal instrument), the European Parliament will be at least partly involved (albeit a little late in the process).

3. Moreover, on substance, the proposals contain a significant part devoted to data protection, some of which being welcome improvements compared to the current situation. In particular, one can mention the measures in favour of victims of identity theft, the extension of Regulation (EC) No 45/2001 to data processing activities of the Commission in the Title VI activities, a better definition of the grounds for alerting individuals for the purpose of refusing entry.

4. It is also obvious that great care has been devoted to the drafting of the proposals; they are complex, but this reflects the inherent complexity of the system they govern. Most of the comments in this opinion aim at clarifying or supplementing provisions, but will not require a complete redrafting.

However, despite this globally positive appreciation, some reservations can be expressed about, in particular, the following:

1. It is in many respects difficult to know what the intention behind the text is; the absence of an explanatory memorandum is highly regrettable. Given the very complex nature of these documents, that would have been a basic requirement. The lack of it in some cases gives the reader no option but guesswork.

2. Moreover, one can only regret there has been no impact assessment study. The fact that the first version of the system is already in place does not justify this, since there are considerable differences between both. Among others, the impact of the introduction of biometric data should have been better thought through.

3. The legal data protection framework is very complex; it is based on the combined application of *lex generalis* and *lex specialis*. It should be ensured that even when a specific legislation is developed, the existing data protection framework in Directive 95/46/EC and Regulation (EC) No 45/2001 remains fully applicable. The combined application of different legal instruments should lead neither to discrepancies between national regimes on fundamental aspects, nor to a watering down of the present level of data protection.

4. Access by many new authorities which do not fit in with the original 'purpose of controls on persons and objects' should be accompanied by more stringent safeguards.

5. The proposals are for a significant part based on other legal instruments which are still in the making (sometimes not even proposed). The EDPS understands the difficulties of legislating in a complex and constantly evolving environment; however, in view of the consequences for the persons concerned and of the legal uncertainty it creates, he deems it not acceptable.

6. There is some fuzziness in the attribution of competences between Member States and the Commission. Clarity is paramount as it is not only necessary for the smooth running of the system, but also a basic requirement to ensure a comprehensive supervision of the system.

1.3. **Structure of the opinion**

The opinion will be structured as follows: it first clarifies the legal framework applicable to the SIS II. It then addresses the definition of the purpose of the SIS II and the elements significantly different from the current system. Point 5 contains comments on the respective roles of the Commission and Member States with regard to the operation of the SIS II. Point 6 concerns the data subject rights while point 7 addresses the supervision, at national and EDPS level, as well as the cooperation between the supervisors. Point 8 proposes some comments and possible amendments on security; points 9 and 10 deal respectively with comitology and interoperability. Finally, a summary of conclusions highlights the principal conclusions for each point.

2. **RELEVANT LEGAL FRAMEWORK**

2.1. **Relevant data protection framework of the SIS II**

The proposals refer to Directive 95/46/EC, Convention 108 and Regulation (EC) No 45/2001 as their legal data protection framework. Other instruments are also relevant.

In order to clarify this context and to remind what the main points of reference for our examination are, it is useful to list the following:

— Respect for private life has been ensured in Europe since the adoption in 1950 of the Convention for the Protection of Human Rights and Fundamental Freedoms (hereinafter: 'ECHR') by the Council of Europe. Article 8 ECHR stipulates 'the right to respect for private and family life'.

  According to Article 8(2) any interference by a public authority with the exercise of this right is only allowed, if it is 'in accordance with the law' and is 'necessary in a democratic society' for the protection of important interests. In the case law of the European Court of Human Rights, these conditions have led to additional requirements as to the quality of the legal basis for interference, the proportionality of any measure, and the need for appropriate safeguards against abuse.

— The right to respect for private life and the protection of personal data have been laid down more recently in Article 7 and 8 of the Charter of the Fundamental Rights of the European Union. According to Article 52 of the Charter, it is recognized that these rights may be subjected to limitations, provided that similar conditions are fulfilled as apply under Article 8 ECHR.

— Article 6(2) of the EU Treaty provides that the Union shall respect fundamental rights, as guaranteed by the ECHR.

The three texts explicitly applicable to the SIS II proposals are the following:

— The Council of Europe Convention No 108 of 28 January 1981 for the Protection of Individuals with regard to Automatic Processing of Personal Data (hereinafter *'Convention 108'*) has developed basic principles for the protection of individuals with regard to the processing of personal data. All Member States have ratified Convention 108. It is applicable also to activities carried out in the framework of the police and judicial areas. Convention 108 is currently the data protection regime applicable to the SIS Convention, together with the Recommendation No R (87) 15 of 17 September 1987 of the Committee of Ministers of the Council of Europe regulating the use of data in the police sector.

— Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (OJ L 281, p. 31). This directive will be referred to as *'Directive 95/46/EC'*. It is worth noting that in most Member State, the national legislation implementing the Directive also covers processing activities carried out in the area of police and justice.

— Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data (OJ L 8, p.1). This regulation will be referred to as *'Regulation (EC) No 45/2001'*.

Interpretation of Directive 95/46/EC and Regulation (EC) No 45/2001 must depend partly on relevant case law from the European Court of Human Rights pursuant to the 1950 European Convention on Human Rights and Fundamental Freedoms (ECHR). In other words, the Directive and the Regulation, in so far as they deal with processing of personal data liable to infringe fundamental freedoms, in particular the right to privacy, must be interpreted in the light of fundamental rights. This also follows from the case law of the European Court of Justice ([1]).

([1]) It is useful in this context to refer to the judgment of the Court of Justice in Österreichischer Rundfunk and Others (Joined Cases C-465/00, C-138/01 and C-139/01, Judgment of 20 May 2003, Full Court, (2003) ECR I-4989). The Court dealt with an Austrian law providing for the transfer of salary details on public sector employees to the Austrian Court of Auditors and their subsequent publication. In its judgment the Court lays down a number of criteria drawn from Article 8 of the European Convention on Human Rights, which should be used when applying Directive 95/46/EC in so far as this directive allows for certain restrictions to the right to privacy.

On 4 October 2005, the Commission issued a 'Proposal for a Council Framework Decision on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters' [1] (hereinafter *'draft Framework Decision'*). This Framework Decision is intended to replace Convention 108 as the legislation of reference for the draft SIS II Decision, which is likely to have an impact on the data protection regime in this context (see below, point 2.2.5).

2.2. **SIS II data protection legal regime**

2.2.1. *General remark*

The legislative basis necessary for governing the SIS II consists of separate instruments; however, as stated in the Recitals, it 'does not affect the principle that the SIS II constitutes one single information system that should operate as such. Certain provisions of these instruments should therefore be identical'.

The structure of the two documents is basically the same, with indeed chapters I-III being almost identical in both texts. The fact that the SIS II is to be seen as a single information system with two different legal bases is also reflected in the — rather complex — data protection regime.

The data protection regime is determined partly in the proposals themselves, as a *'lex specialis'*, complemented by a different legislation of reference (*'lex generalis'*) for each sector (Commission, Member States in first pillar, Member States in third pillar).

This structure raises the question of how to deal with specialised sets of rules in their relationship to general law. In this case, the EDPS considers the particular rule an application of the general rule. As a consequence, the *lex specialis* must always be in conformity with the *lex generalis*; it elaborates (specifies or adds to) the *lex generalis* but is not conceived as an exception from it.

As to the question of which rule should be applied in specific cases, the principle is that the *lex specialis* applies in priority; but wherever it is silent or unclear, reference should be made to the *lex generalis*.

There are, according to this structure three different combinations of *lex generalis* and *lex specialis*. It could be summarized as follows.

2.2.2. *Applicable regime for the Commission*

Where the Commission is involved, Regulation (EC) No 45/2001 applies, including the role of the EDPS, whether the activities are carried out in the framework of the first (proposed Regulation) or third pillar (proposed Decision). Recital 21 of the proposed Decision states that: 'Regulation (EC) No 45/2001 (…) applies to the processing of personal data by the Commission when such processing is carried out in the exercise of activities all or part of which fall within the scope of Community law. Part of the processing of personal data in the SIS II is within the scope of Community law'.

There are practical reasons for this: it would indeed be extremely difficult, as far as the Commission is concerned, to determine if the data are processed in the framework of activities falling under first or third pillar legislation.

Moreover, applying one legal instrument to all activities by the Commission in the context of the SIS II, not only makes more sense from a practical point of view, but also improves consistency (ensuring, according to Recital 21 of the proposed Regulation a 'consistent and homogeneous application of the rules regarding the protection of individuals' fundamental rights and freedoms with regard to the processing of personal data'). Therefore, the EDPS welcomes the recognition by the Commission that Regulation (EC) No 45/2001 applies to all data processing activities of the Commission in SIS II.

2.2.3. *Applicable regime for the Member States*

The situation concerning Member States is more complex. The processing of personal data in application of the proposed Regulation is governed by the proposed Regulation itself as well as by Directive 95/46/EC. The reading of Recital 14 of the proposed Regulation makes it very clear that the Directive must be considered as the *lex generalis*, while the SIS II Regulation will be the *lex specialis*. This has a number of consequences that will be detailed hereunder.

As to the proposed Decision, the data protection legal instrument of reference (*lex generalis*) is the Convention 108, which can make an important difference between the data protection regimes in first and third pillar on some points.

2.2.4. *Impact on the level of data protection*

As a general comment on this architecture of data protection, the EDPS underlines the following:

— The application of the proposed Regulation as a *lex specialis* of Directive 95/46/EC (and similarly, of the proposed Decision as a *lex specialis* of the Convention 108) should never lead to a watering down of the level of data protection ensured under the Directive or Convention. The EDPS will make recommendations to this effect (see for instance the right to remedies).

[1] (COM (2005) 475 final).

— Similarly, the combined application of legal instruments can not have as a result that the level of data protection ensured under the current Schengen Convention will be lowered (see for instance the remarks hereunder about Article 13 of Directive 95/46/EC).

— The application of two different instruments, however necessary because of the framework of European law, should not lead to unjustified discrepancies between the data protection of the individuals concerned according to the type of data processed about them. This is to be avoided as much as possible. The recommendations made hereunder will also strive to improve consistency as much as possible (see for instance the powers of the national supervisory authorities).

— The legal framework is so complex that it is very likely to engender some confusion in the practical application. It is in some cases difficult to see how *lex generalis* and *lex specialis* interact, and it would be useful to clarify this in the proposals. Moreover, in this complex legal environment, the suggestion made by the JSA Schengen in its 'opinion on the proposed legal basis for the SIS II' (27 September 2005) to develop a 'vademecum' listing all the rights existing in relation to the SIS II and providing a clear hierarchy of applicable legislation is very useful.

In conclusion, the present opinion will strive to ensure a high level of data protection, consistency and clarity to provide the data subject with the necessary legal certainty.

2.2.5. *Impact of the Draft Framework Decision on Data Protection in Third Pillar*

The Convention 108 as the data protection instrument of reference for the draft SIS II Decision will be replaced by the Framework Decision on data protection in the third pillar ([1]). This is not mentioned in the proposal, but follows from the proposed framework decision. Its Article 34.2 states that 'Any reference to the Convention No 108 of the Council of Europe of 28 January 1981 for the protection of individuals with regard to automatic processing of personal data shall be construed as a reference to this Framework Decision'. The EDPS will issue in the coming weeks an opinion on the draft Framework Decision and will not analyse in details its content in this opinion. However, wherever the application of the Framework Decision is likely to have a significant impact on the SIS II data protection regime, this will be mentioned.

([1]) It will also replace the general data protection regime of the Schengen Convention (Articles 126 to 130 of the Schengen Convention). This regime does not apply to the SIS.

2.2.6. *Application of Article 13 of Directive 95/46/EC and Article 9 Convention 108*

Article 13 of Directive 95/46/EC and Article 9 of the Convention 108 provide for the possibility for Member States to take legislative measures to restrict the scope of obligations and rights provided for by them, when such a restriction constitutes a necessary measure to safeguard other important interests (e.g. national security, defence, public security) ([2]).

The Recitals of both the proposed Regulation and proposed Decision mention that this possibility could be used by Member States when implementing the proposals at national level. A double test should be applied in this case: the application of Article 13 of the Directive 95/46/EC must be in compliance with Article 8 ECHR and should not lead to a diminution of the present data protection regime.

It is even the more crucial in the case of SIS II, since the system must have a predictable character. As Member States are sharing data, there must be a possibility to know with reasonable certainty how they will be processed at national level.

There is in particular one worrying element with regard to this, where the proposals would lead to a lowering of the current data protection level. Article 102 of the Schengen Convention provides for a system where the use of the data is strictly regulated and restricted, even in national legislation ('Any use of the data which does not comply with paragraphs 1 to 4 shall be considered as misuse under the national law of the Contracting Party'). Both Directive 95/46/EC and Convention 108, however, provide that exceptions, inter alia, to the principle of purpose limitation can be introduced in national legislation. If this is done, it would represent a discrepancy with the current system in the Schengen Convention, where national legislation can not deviate from the core principle of purpose and use limitation.

The adoption of the Framework Decision would not change this observation: the problem is much more to maintain a strict purpose limitation principle for the processing of SIS II data than to ensure that data would be processed in compliance with the Framework Decision.

([2]) A Member State using this option to restrict rights may only do so in compliance with Article 8 ECHR, as mentioned before.

The EDPS suggests to introduce in the SIS II proposals (namely Article 21 of the proposed Regulation and Article 40 of the proposed Decision) a provision to the same effect as the current Article 102.4 of the Schengen Convention, limiting the possibility for Member States to provide for use of the data not foreseen in the SIS II texts. Another possibility is to restrict explicitly in the proposed Decision and proposed Regulation the scope of the exceptions that can be used under Article 13 Directive or Article 9 Convention, laying down, for instance, that Member States can only restrict the rights of access and information, but not the data quality principles.

3. PURPOSE

According to Article 1 of the two documents ('establishment and general objective of the SIS II'), the SIS II is established to 'enable competent authorities of the Member States to exchange information for the purpose of controls on persons and objects', and shall 'contribute to maintaining a high level of security within an area without internal border controls between Member States'.

The purpose of the SIS II is worded in rather broad terms; the provisions mentioned above are not in themselves a precise indication of what is covered (meant) by this objective.

The objective of the SIS II seems much broader than the objective of the current SIS as laid down in Article 92 of the Schengen Convention, which referred specifically to '(…) access alerts on persons and property for the purposes of border checks and other police and customs checks (…) and (concerning Article 96 alerts) for the purpose of issuing visas, residence permits and the administration of legislation on aliens (…)'.

This broader purpose also derives from the addition to the SIS II of new functionalities and accesses which do not fit into the original purpose of controls on persons and objects, but more into an investigative tool. In particular, access is foreseen for authorities who will use the SIS II data for their own purposes, and not for the realisation of the SIS II purposes (see below); interlinking of alerts will be generalized while this represents a typical feature of a police investigative tool.

There are also questions as to the biometric search engine which is to be developed in the coming years, allowing for searches in the system, which exceed the needs of a control system.

In conclusion, the proposals have a much broader scope than the existing framework. This requires additional safeguards. In this regard, the EDPS will focus his analysis not so much on the broad definition in Article 1 as such, but on the functionalities and other constitutive parts of the SIS II.

4. SIGNIFICANT CHANGES IN THE SIS II

This chapter will focus first on the new elements brought in by the SIS II, namely the introduction of biometrics, the new conception of access, with special attention to access by Europol and Eurojust, to authorities in charge of vehicle registration, the interlinking of alerts, and access by different authorities to immigration data.

4.1. Biometrics

The SIS II proposals introduce the possibility to process a new category of data which deserves specific attention: biometric data. As already underlined in the EDPS opinion on the Visa Information System [1], the inherently sensitive nature of biometric data requires specific safeguards which have not been introduced in the SIS II proposals.

As a general comment, the tendency to use biometric data in EU wide information systems (VIS, EURODAC, Information System on driving licences etc.) is growing steadfastly, but is not accompanied by a careful consideration of risks involved and required safeguards.

This need for a deeper reflection has been also highlighted in the recent resolution on biometrics issued by the International Conference of Data Commissioners in Montreux [2]. Until now, the added value for developing standards has been only focused on the growing interoperability between systems and not on the improvement of the quality of the biometric processes.

[1] Opinion of the EDPS on the Proposal for a Regulation of the European Parliament and of the Council concerning the Visa Information System and the exchange of data between Member States on short stay visas, 23 March 2005, pt 3.4.2.

[2] 27th International Conference of Data Protection and Privacy Commissioners, Montreux, 16 September 2005, Resolution on the use of biometrics in passports, identity cards and travel documents.

It would be useful to build a set of common obligations or requirements related to the specificity of such data as well as a common methodology for their implementation. These common requirements could contain in particular the following elements (the need of which is illustrated by the SIS II proposals):

— **Targeted impact assessment:** It has to be underlined that the proposals have not been subjected to an impact assessment on the use of biometrics ([1]).

— **Emphasis on the enrolment process:** The source of biometric data and the way they will be collected are not detailed. Enrolment is a critical step in the overall process of biometric identification and cannot be only defined by annexes or further sub-group discussions as it will directly condition the end-result of the process i.e. the level of False Rejection Rate or False Acceptance Rate.

— **Highlight the level of accuracy:** The use of biometrics for identification (comparison of one to many) presented in the proposal as a future implementation of a 'biometrics search engine' are more critical because the results of this process are less accurate than the use for authentication or control (one to one comparison). Biometric identification should not therefore constitute the unique way of identification or unique access key to further information.

— **Fallback procedure:** Readily available fallback procedures shall be implemented in order to respect the dignity of persons who could have been wrongly identified and to avoid transferring onto them the burden of the system imperfections.

The use of biometric data without a proper preliminary assessment also reveals an overestimation of the reliability of biometrics. Biometric data are 'live' data which evolve with time; the samples which are stored in the database constitute only a snapshot of a dynamic element. Its permanency is not absolute and need to be controlled. The accuracy of biometrics always has to be put into perspective of other elements as it will never be absolute.

The possible use of SIS II data for investigation purposes entails serious risks for the data subject if one gives an increased or over-estimated role to biometric evidence as it has been illustrated in previous cases ([2]).

Therefore, the proposals should recognise and raise awareness on the real capabilities of biometrics for identification purposes.

4.2. **Access to SIS II data**

4.2.1 *A new vision of access*

The authorities with access to SIS data are defined for each alert. In principle, a double test is applied for granting access to the SIS data: access must be granted to authorities in full compliance with the general purpose of the SIS and with the specific purpose of each alert.

This follows from the definition of alerts found both in the proposed Regulation and the proposed Decision (Art.3.1.a of both instruments: *'Alert' means a set of data entered in the SIS II allowing the competent authorities to identify a person or an object, in view of a specific action to be taken*). Article 39.3 of the proposed Decision reinforces that view by stipulating that *'the data referred to in paragraph 1 shall only be used for the purpose of identifying a person in view of a specific action to be taken in accordance with this decision'*. In this respect, the SIS II still has the features of a hit-no hit system, where each alert is inserted for a specific purpose (surrender, refusing entry,…).

The authorities with access to the SIS data have a de facto use limitation for these data, since they can in principle only have access to them to perform a specific action.

However, some accesses provided for in the new proposals are not consistent with this logic: indeed, they aim at providing the authority with information, but not at allowing it to identify a person and take the action foreseen in the alert.

([1]) The assessment could be based on the so-called seven pillars of biometric wisdom *in*'Biometrics at the frontiers: Assessing the impact on Society' IPTS, DG-JRC, EUR 21585 EN, part 1.2, page 32.

([2]) In June 2004, a Lawyer from Portland (US) was jailed for two weeks because the FBI successfully matched his fingerprint with one found in the Madrid terrorist bombing (on the plastic bag which contained the detonator). It was finally demonstrated that the matching process was flawed and resulted to a misinterpretation.

More specifically, this concerns:

— access to immigration data by asylum authorities;

— access to immigration data by authorities in charge of granting refugees status;

— access to alerts on extradition, discreet surveillance and stolen documents for seizure for Europol;

— access to data on extradition and localisation for Eurojust.

All these authorities share the same characteristics with regard to the SIS II data:

they are not able to take the specific action mentioned by the definition of the alerts. Access is granted to them as a source of information for their own purposes.

Even between these authorities, there is a distinction to be made between the ones having access for their own purposes, but with a rather specific objective, and the ones (namely Europol and Eurojust), for which there is no specification at all of the purpose of the access. Asylum authorities, for instance have access for a specific purpose, even if it is not the purpose mentioned in the alert. They can have access to immigration data 'for the purpose of determining whether an asylum applicant has stayed illegally in another Member State'. Europol and Eurojust, however, have access to the data contained in certain categories of alerts, 'which is necessary for the performance of their tasks'.

To summarize, access to SIS II data is granted in three cases:

— access for realisation of the alert;

— access for a purpose other than SIS II, but well circumscribed in the proposals;

— access for a purpose other than SIS II, but not precisely described.

The EDPS takes the view that, the more general the purpose for access, the more stringent the safeguards which need to be implemented should be. The general safeguards are detailed hereunder; then, the specific situation of Europol and Eurojust will be addressed.

4.2.2 *Conditions for granting access*

1. Access can in any case be granted only when it is compatible with the general purpose of the SIS II, and consistent with its legal basis.

   This means, in practice that access to immigration data pursuant to the proposed Regulation must support the implementation of policies linked to the movement of persons part of the Schengen acquis.

   Similarly, access to alerts laid down by the Decision shall aim at supporting operational cooperation between police authorities and judicial authorities in criminal matters.

   In this regard, the EDPS draws the attention to the chapter related to access to SIS II by services responsible for issuing registration certificates (see below, pt 4.6).

2. The need for access to SIS II data must be demonstrated, as well as the impossibility or great difficulty to obtain the data by other, less intrusive means. This should have been done in an explanatory memorandum, whose absence is, as already said, very regrettable.

3. The use that will be made of data must be defined explicitly and restrictively.

   For instance, asylum authorities have access to immigration data 'for the purpose of determining whether an asylum applicant has stayed illegally in another Member State'. Europol and Eurojust, however, have access to the data contained in certain categories of alerts, 'which is necessary for the performance of their tasks: this is not sufficiently detailed (see below)'.

4. The conditions of the access must be well defined and restricted. In particular, only the services inside these organisations which have to deal with the SIS II data, should get an access to it. This obligation laid down in Article 40 of the proposed Decision and Article 21.2 of the proposed Regulation should be supplemented by an obligation for the national authorities to keep an up-to-date list of persons entitled to access the SIS II. The same should apply to Europol and Eurojust.

5. The fact that these authorities are granted access to SIS II data can never be a ground for entering or maintaining data in the system if they are not useful for the specific alert they are part of. New categories of data may not be added because they would benefit other information systems. For example, Article 39 of the proposed Decision provides for the introduction in alerts of data concerning the issuing authority. These data are not needed to perform an action (arrest, surveillance,…), and the only reason why they could be introduced is probably to benefit Europol or Eurojust. A clear rationale for the processing of this data should be provided.

6. The retention period of the data may not be extended where it is not necessary for the purpose for which the data was entered. That means that even if Europol or Eurojust have an access to these data, this is not sufficient ground for maintaining them in the system (for instance, once a wanted person has been extradited, the data should be deleted, even if they could be useful for Europol). Here again, careful supervision will be needed to ensure this is applied by the national authorities.

4.2.3 *Access by Europol and Eurojust*

a. *Grounds for access*

The access by Europol and Eurojust to some SIS data has already been debated before their introduction by the Council Decision of 24 February 2005 ([1]). Among all the authorities having access for their own purposes, they benefit from an access granted in the most open terms. Although the use of these data is described in Chapter XII of the Decision, the grounds for granting access in the first place are not sufficiently developed. This is even the more so considering that Europol and Eurojust's tasks are likely to evolve over time.

The EDPS urges the Commission to define restrictively the tasks for the performance of which access by Europol and Eurojust would be justified.

b. *Restriction of data*

In order to avoid 'fishing expeditions' by Europol and Eurojust, and to make sure they only access data 'necessary for their tasks', the JSA Schengen in its opinion of 27 September 2005 on the SIS II proposals, suggested to restrict Europol and Eurojust access to data about individuals whose name already appear in their files. This would guarantee that only alerts relevant for them are consulted. The EDPS supports this recommendation.

c. *Security aspects*

The EDPS welcomes the obligation of logging all transactions made in connection by Europol and Eurojust, as well as the interdiction of copying or downloading parts of the system.

Article 56 of the proposed Decision envisages 'one to two' access points for Europol and Eurojust. However understandable it could be for a Member State to need more than one access point, due to a decentralised situation of its competent authorities, the status and activities of Europol and Eurojust do not justify this request. It has to be underlined as well that from a security point of view, the multiplication of access points increases the risk of misuse and should therefore be precisely justified with more consistent elements. Therefore, in the absence of convincing argumentation, the EDPS suggests to grant only one access point in the cases of Europol and Eurojust.

4.3. **Interlinking of alerts**

Article 26 of the Regulation and Article 46 of the Decision provide that Member States may create links between alerts in accordance with their national legislation, in order to establish a relationship between two or more alerts.

Although links between alerts can certainly be useful to controls (for instance, an arrest warrant on a car thief can be linked to a stolen vehicle), the introduction of links between alerts is a very typical feature of a police investigative tool.

Interlinking of alerts can have a major impact on the rights of the person concerned, since the person is no longer 'assessed' on the basis of data relating only to him/her, but on the basis of his/her possible association with other persons. Individuals whose data are linked to those of criminals or wanted persons are likely to be treated with more suspicion than others. Interlinking of alerts furthermore represents an extension of the investigative powers of the SIS because it will make possible the registration of alleged gangs or networks (if, for instance, data on illegal immigrants are linked with data of traffickers). Finally, since the establishment of links is left to national legislation, it has as a possible consequence that links which are illegal in one Member State can be established by another one, thus feeding 'illegal' data into the system.

([1]) Council Decision 2005/211/JHA of 24 February 2005 concerning the introduction of some new functions for the Schengen Information System, including the fight against terrorism, OJ L 68/44, 15.3.2005

The Council Conclusions of 14 June 2004 on the functional requirements on the SIS II stated that each link must have a clear operational requirement, be based on a clearly defined relationship and comply with the proportionality principle. Moreover, it may not affect the access rights. Anyway, since the interlinking of alerts constitutes a processing operation, it must comply with the provisions of the national legislation implementing Directive 95/46/EC and/or Convention 108.

The proposals reiterate that the existence of links cannot change the access rights (indeed, it would otherwise give access to data the processing of which would not be lawful under national legislation, in breach of Article 6 of the Directive).

The EDPS stresses the importance of a strict interpretation of Article 26 of the proposed Regulation and Article 46 of the proposed Decision: one way to ensure this is to make clear that authorities with no right of access to certain categories of data not only cannot have access to links to those categories, but that they should not even be aware of the existence of these links. The visualisation of the links must be impossible where there is no access right to the linked data.

Moreover, the EDPS would like to be consulted on the technical measures to guarantee this.

4.4. **Alerts for the purpose of refusing entry**

4.4.1. *Grounds for inclusion*

The use of 'alerts issued in respect of third country nationals for the purpose of refusing entry' (Article 15 of the Regulation) has a significant impact on the freedoms of the individual: an individual reported under this provision has no more access to the Schengen area for several years. This has been until now the most often used alert in terms of the number of persons reported. Seeing the consequences of this alert, as well as the number of persons concerned, great care must be taken in its conception, as well as in its implementation. Although this is also true concerning other alerts, the EDPS will devote a specific chapter to this alert, because it poses specific problems concerning the grounds for inclusion.

The new alert for refusing entry presents improvements with regards to the present situation, but is also not completely satisfactory, as it is based in good part on instruments which have not yet been adopted or even proposed.

The improvements reside in a more precise description of the grounds of inclusion of the data. The current wording of the Schengen Convention has led to a situation where there were significant differences between Member States in terms of the number of persons reported under Article 96 of the Convention. The JSA Schengen has conducted a comprehensive study [1] on that matter and came up with recommendations that 'policy makers should consider harmonising the reasons for creating an alert in the different Schengen States'.

The proposed Article 15 is more detailed in its drafting, which is to be welcomed.

Moreover, Article 15.2 gives also a list of cases where persons cannot be alerted because they are legally residing on the territory of a Member State, in application of different statuses. Although it could be deduced from the present Schengen Convention, the practice has shown that the application of this mechanism also was subject to variation between Member States. Therefore, clarification is a positive element.

However, this provision is also subject to serious criticism, as it is based for an important part on a not yet adopted text, namely the Directive 'on Return'.

Since the adoption of the SIS II proposals, a 'Directive on common standards and procedures in Member States for returning illegally staying third-country nationals' has been proposed by the Commission (on 1 September 2005), but as long as this text is not final, it cannot be considered as a valid ground for entering data into a system. It constitutes, in particular a breach of Art. 8 ECHR, since an intrusion in the privacy of individuals should be justified by — inter alia — a clear and accessible legislation.

Therefore, the EDPS urges the Commission to either withdraw this provision, or redraft it in a way, based on existing legislation, that allows the individuals to know which measures exactly the authorities can take regarding him/her.

4.4.2. *Access to Article 15 alerts*

Article 18 lays down which authorities have access to these alerts and for which purposes. Article 18 (1) and (2) determines which authorities have access to alerts entered on the basis of the Directive on Return. The same commentary as above applies.

[1] Report of the Schengen Joint Supervisory Authority on an inspection of the use of Article 96 alerts in the Schengen Information System, Brussels, 20 June 2005.

Article 18 (3) of the proposed Regulation grants access to authorities responsible for granting refugee status, pursuant to a Directive which has not yet been even proposed. In the absence of an available text, the EDPS must reiterate the comments made here above.

4.4.3. *Retention period of Article 15 alerts*

The alert must, according to Article 20 not be kept longer than the period of refusal of entry laid down in the decision (of removal or return). This is consistent with data protection rules. Moreover, it will be erased automatically after five years, unless the Member State having entered the data in the SIS II decides otherwise.

Adequate supervision at national level should ensure that there is no automatic unjustified extension of the retention period, and that the Member States erase the data before the five year term if the period of refusal of entry happens to be shorter.

4.5. **Retention periods**

Although the principle of retention remains the same (as a general rule, an alert should be erased from the SIS II as soon as the action requested by the alert is taken), the proposals will have as a result that the retention period for the alerts has been generally extended.

The Schengen Convention provided for a review of the need for continued storage of the data no later than three years after they were entered (or one year in the case of data entered for discreet surveillance). The new proposals foresee an automatic deletion (with possibility to object for the issuing Member State) after 5 years for immigration data, 10 years for data on arrest, missing persons and persons wanted for judicial procedures, and 3 years for persons to be put under discreet surveillance.

Even though in principle, the Member States will have to delete the data when the purpose of the alert is met, this amounts to a significant increase of the maximum retention period (in most cases, tripling), without any sort of justification by the Commission. In the case of immigration data one can only venture a guess that the 5 years duration is linked with the duration of the entry ban as proposed in the draft Directive on Return. In all other cases, there is no rationale that the EDPS is aware off.

The potential impact on the data subjects being reported in the SIS can have considerable consequences on the lives of the persons concerned. This is especially worrying in the case of alerts on persons for discreet surveillance or specific checks, since these alerts may be issued on the basis of suspicions.

The EDPS would like to see serious justification for this extension of data retention periods. If there is no convincing justification, he suggests reducing them to their current duration, insisting particularly on the case of alerts for the purpose of discreet surveillance or specific checks.

4.6. **Access by authorities in charge of issuing vehicle registration certificates**

The main issue resides in the choice of a more than questionable legal basis. The Commission fails to make a convincing case for the use of a First Pillar 'transport' legal basis for a measure which would allow access to the SIS by administrative authorities for the purposes of preventing and fighting crime (trafficking of stolen vehicles). The need for a strong justification and a solid legal basis for granting access to the SIS II was detailed in point 4.2.2 of the present opinion.

The EDPS refers to the comments on this subject made by the JSA Schengen in its opinion on the proposed legal basis for the SIS II. In particular, the suggestion made by the JSA Schengen to amend the proposed Decision in order to include in it this access is to be followed.

5. **ROLE OF THE COMMISSION AND THE MEMBER STATES**

A clear description and allocation of responsibilities in the context of the SIS II is paramount, not only for a smooth functioning of the system, but also from a supervision point of view. The distribution of supervisory competences will follow from the description of responsibilities, hence a need for absolute clarity.

5.1. **Role of the Commission**

The EDPS welcomes chapter III of both proposals which describes the role and responsibilities of the Commission for SIS II (as a role of 'operational management'). Such clarification was not present in the VIS proposal. However this chapter alone does not define exhaustively the role of the Commission. Indeed, as discussed in chapter 9 of this opinion, the Commission is also involved in the implementation and the management of the system through the comitology procedure.

In terms of data protection, the Commission has a role that is recognised already in the VIS and Eurodac systems, that of a responsible for operational management. In combination with its major role in the development and maintenance of the system, this should be seen as the role of a sui generis controller. It is, as already said in the EDPS'opinion on the VIS, much more than that of a processor, but also more limited than that of a normal controller, since the Commission has no access to the data processed in the SIS II.

As the SIS II will be built on complex systems, amongst which some rely on emerging technologies, the EDPS insists upon reinforcing the responsibility of the Commission in maintaining the systems up-to-date by implementing the Best Available Technologies related to security and data protection.

It should be added therefore in the Article 12 of the proposals that the Commission should regularly propose the implementation of new technologies which represent the state of the art in this field and which will enhance data protection and security levels, as well as facilitate the tasks of the national authorities which have access to these data.

5.2. **Role of the Member States**

The situation of Member States is not really clear, as it is rather difficult to know which authority(ies) is(are) going to be the data controller(s).

The proposals describe a role for SIS II National Office (to ensure competent authorities' access to the SIS II) as well as for SIRENE authorities (to ensure the exchange of all supplementary information). Member States also have to ensure the functioning and security of their 'NS' ('National System'). It is not clear if this last responsibility is to be borne by one of the above mentioned authorities. In any case, clarification is needed in this regard.

In terms of data protection, the Commission and the Member States should be considered as joint controllers, each with specific responsibilities. The recognition of these complementary missions is the only way to leave no area of the SIS II activities unsupervised.

6. **DATA SUBJECTS RIGHTS**

6.1. **Information**

6.1.1. *Proposed Regulation*

Article 28 of the proposed Regulation foresees the right of information of the data subject, following mainly Article 10 of Directive 95/46. This is a welcome change compared to the current situation, where there is no right of information explicitly foreseen in the Convention. There is, however some room for improvement, on the following points.

Some information should be added to the list, because it would contribute to ensuring a fair treatment of the data subject ([1]). This information should concern the retention period of the data, the existence of the right to request a review or appeal of the decision to issue an alert (in some cases, see Article 15 (3) of the proposed Regulation), the possibility to obtain assistance from the data protection authority, and the existence of remedies.

There is no indication in the proposed Regulation as to the moment when the information should be provided. This could make the rights of the data subject impossible to exercise. In order to make these rights effective, the Regulation should provide for a precise moment where the information should be given, depending from the authority who issued the alert.

A practical solution would be to add information about the alert in the decision which is the ground for the alert in the first place: either a judicial or administrative decision based on a threat to public policy (….) or a return decision or removal order accompanied by a re-entry ban. This should be added to Article 28 of the Regulation.

6.1.2. *Proposed Decision*

Article 50 of the Decision stipulates that information is given on request of the data subject and states the possible grounds for refusing to grant this information. Limitations to this right are obviously understandable, considering the nature of the data and the context in which they are processed.

However, the right of information should not be subjected to a request of the data subject (that would actually rather be the definition of a request for access). One can suppose that the need to 'request' information was justified by the cases where the data subject cannot be informed because he is not located.

This would be better addressed by adding an exception to the right of information in cases where the provision of information proves impossible or involves a disproportionate effort. Article 50 of the Decision should be amended accordingly.

([1]) In the same sense, see EDPS Opinion on the establishment of the Visa Information System, pt 3.10.1.

This solution would also be consistent with the application of the draft Framework Decision on Data protection in third pillar.

6.2. **Access**

The proposed Regulation and Decision both impose deadlines for answering requests for access, which is a positive evolution. However, since the procedure for exercising the right of access is defined at national level, one can wonder how the delays imposed in the proposals can interact with the existing procedures, especially if the Member States have shorter deadlines to answer a request for access. It should be made clear that the deadlines which are the most favourable to the data subject should be applied.

6.2.1. *Proposed Regulation*

It is worth noting that the restrictions to the right of access ('shall be refused if this is indispensable for the performance of a lawful task in connection with the alert or for the protection of rights and freedoms of third parties') which currently exist in the Schengen Convention do not figure in the proposed Regulation.

However, this is probably due to the applicability of the Directive 95/46/EC which foresees (in its Article13) the possibility to implement exceptions in national legislations. In any case, it should be pointed out that the use of Article 13 in national legislation for restricting the right of access should always be in compliance with Article 8 ECHR, only in limited cases.

6.2.2. *Proposed Decision*

The proposed Decision takes up the limitation to the access right as in the Schengen Convention. The proposed Framework Decision contains in essence the same limitations to the right of access; so the adoption of this instrument would not make a significant difference in this.

Since in several Member States, access to law enforcement data is 'indirect' (which means exercised via the national data protection authority), it should be useful to provide for an obligation of data protection authorities to cooperate actively in the exercise of the right of access.

6.3. **Right to review or appeal the decision to issue an alert**

Article 15 (3) of the Regulation institutes a right to review or appeal before a judicial authority with respect to the decision to issue an alert, when this decision is taken by an administrative authority. This is a welcome addition, compared to the current Schengen Convention.

This underlines the need for complete and timely information of the data subject as mentioned in point 6.1 above: without this information this new right would remain theoretical.

6.4. **Remedies**

Article 30 of the proposed Regulation and Article 52 of the proposed Decision provide for the right to bring an action or a complaint before the courts of any Member State, if the data subject is refused the right of access, rectification or erasure of data, to obtain information or reparation.

The wording ('any person in the territory of a Member State') suggests that the complainant must be physically on the territory to bring his action before courts. This territorial limitation is not justified and could make the right to remedies ineffective, as very often, the complainant is likely to introduce an action precisely because he is not granted access to the Schengen territory. Moreover, as far as the proposed Regulation is concerned, since the Directive is the *lex generalis*, its Article 22 must be taken into account; it stipulates that 'every person' has a right to a judicial remedy, irrespective of his place of residence. The proposed Framework Decision does not contain either a territorial limitation. The EDPS suggests dropping the territorial limitation in Article 30 and Article 52.

7. **SUPERVISION**

7.1. **Introductory remark: sharing of responsibilities**

The proposals share out the supervisory task between national supervisory authorities [1], and the EDPS, each for its own scope. This is consistent with the approach of the proposals to applicable law and responsibilities for the operation and use of the SIS II, and with the need for an effective supervision.

The EDPS therefore welcomes this approach in Article 31 of the proposed Regulation and Article 53 of the proposed Decision. However, for a better understanding and a clarification of the respective tasks, the EDPS proposes to split each article into several provisions, each of them dedicated to a level of supervision as had been properly done in the VIS proposal.

[1] The supervisory authorities for Europol and Eurojust are also involved, but to a lesser extent.

7.2. **Supervision by national data protection authorities**

Pursuant to Article 31 of the proposed Regulation and Article 53 of the proposed Decision, each Member State must ensure that an independent authority monitors the lawfulness of the processing of SIS II personal data.

Article 53 of the proposed Decision adds a right for the individual to ask the supervisory authority to check the lawfulness of the processing of the data concerning him. A similar provision has not been included in the proposed Regulation since the Directive applies as a *lex generalis*. Therefore, it must be considered that national data protection authorities can exercise, with regard to the SIS II all the competences conferred to them by Article 28 of the Directive 95/46/EC, including checking the lawfulness of a data processing. Article 31.1 of the Regulation is a clarification on their mission but cannot constitute a limitation of these powers. The recognition of these competences should be clarified in the text of the proposed Regulation.

As to the proposed Decision, it recognises more extensive duties to national supervisory authorities because its *lex generalis* is different. However, the situation where supervisory authorities would have different missions and competences according to the category of processed data is not sound, and very difficult to manage in the practice. Therefore, it should be avoided, either by recognising these authorities the same powers in the text of the proposed Decision itself, or by referring to another *lex generalis* (namely the Framework Decision on Data Protection in Third Pillar) giving more competences to the data protection authorities.

7.3. **Supervision by the EDPS**

The EDPS monitors that the data processing activities of the Commission are carried out in accordance with the proposals. Similarly, the EDPS should be able to exercise all his competences under Regulation (EC) No 45/2001, taking into account, however, the limited powers of the Commission with regard to the data themselves.

It is useful to add that, according to Article 46 (f) of Regulation (EC) No 45/2001, the EDPS 'shall cooperate with the national supervisory authorities to the extent necessary for the performance of their respective duties'. The cooperation with Member States in the supervision of the SIS II does not stem only from the proposals, but also from Regulation (EC) No 45/2001.

7.4. **Joint supervision**

The proposals also recognise the need to coordinate the supervisory activities of the different authorities involved. Article 31 of the proposed Regulation and Article 53 of the proposed Decision stipulate that 'the national supervisory authorities and the European Data Protection Supervisor shall cooperate actively with each other. The European Data Protection Supervisor shall convene a meeting for that purpose at least once a year'.

The EDPS welcomes this proposal which contains in essence the necessary elements to create the cooperation — which is indeed crucial — between the authorities in charge of supervision at national and European level. It should be underlined that the proposals provide for a meeting at least once a year, but that it is to be considered as a minimum.

These provisions (Article 31 of the proposed Regulation and Article 53 of the proposed Decision) could however benefit from some clarifications of the content of that coordination. The existing JSA has the competence to examine difficulties of interpretation or application of the Convention, to study problems that may occur with the exercise of independent supervision or of the right of access, and to draw up harmonised proposals for joint solutions to existing problems.

The new proposals cannot lead to a watering down of the existing scope of the common supervision. If it is clear that data protection authorities can exercise with regard to the SIS II all the supervisory competences they are endowed with under the Directive, the cooperation of these authorities can cover broad aspects of the supervision of the SIS II, including the tasks of the existing JSA as developed in Article 115 of the Schengen Convention.

However, in order to make this absolutely clear, it would be useful to reaffirm this explicitly in the proposals.

8. **SECURITY**

The management of and respect for an optimal security level for the SIS II constitutes a fundamental requirement for ensuring an adequate protection of personal data stored in the database. In order to obtain this satisfactory level of protection, proper safeguards have to be implemented for handling the potential risks related to the infrastructure of the system and to the persons involved. This subject is now discussed in various parts of the proposal and deserves some improvement.

Articles 10 and 13 of the proposal contain various measures for data security and specify the kind of misuses that need to be prevented. The EDPS welcomes that provisions on systematic (self-)auditing of security measures have been included in these articles.

However Article 59 of the proposed Decision and Article 34 of the proposed Regulation, which provide for monitoring and evaluation, should not only concern the aspects of output, cost-effectiveness and quality of services, but also compliance with legal requirements, especially in the field of data protection. The EDPS therefore recommends that the scope of these articles is extended to monitoring and reporting on the lawfulness of processing.

Moreover, in complement to Article 10 (1) (f) or Article 18 of the proposed Decision and Article 17 of the proposed Regulation concerning the duly authorised staff who has access to the data, it should be added that Member States (as well as Europol and Eurojust) should ensure that precise user profiles are available (that should be kept at the disposal of the national supervisory authorities for checks). In addition to these user profiles, a complete list of user identities has to be made and kept permanently up-to-date by Member States. The same applies *mutatis mutandis* to the Commission.

These security measures are completed by monitoring and organisational safeguards. Article 14 of the proposals describes the conditions and the purposes for which records of all data processing operations have to be kept. These records shall not only be stored for monitoring data protection and ensuring data security but also for consolidating the regular self-auditing of the SIS II requested by Article 10. The self-auditing reports will contribute to the effective execution of the tasks of the supervisory authorities that will be able to identify the weakest spots and to focus on them during their own auditing procedure.

As it was stated earlier in this opinion, the multiplication of access points to the system needs to be carefully justified as it automatically increases the risks of abuses. A concrete demonstration of the need for a second access point should therefore be requested by Article 4 (1) (b) of the proposals.

The proposals do not clearly explain the need for national copies of the central system and trigger serious concerns regarding the overall level of risk and security of the system, such as:

— The multiplication of copies increases the risks of abuse (especially taking into account the presence of new data like biometric data);

— The data concerned by these copies are not well defined;

— The accuracy, quality, and availability requirements of the article 9 constitute great technical challenges and therefore increase the cost according to the state of the art of the available technology;

— The supervision by the national authorities of these copies will request additional human and financial resources which might not be always available.

In view of the risks involved, the EDPS is neither convinced of the necessity (considering the available technologies) nor of the added value of the use of national copies. He recommends dropping the possibility for Member States to use national copies.

However, if the national copies are to be developed, the EDPS reminds that a strict purpose limitation principle must be applied to their national use. Similarly, the national copy may never be queried in other ways than the central database.

The lawfulness of the personal data processing operation is based on the strict respect of data security and data integrity. The EDPS will monitor in an efficient way these processes, if he can not only monitor the security of data, but also their integrity through the analysis of the available logs. It is thus necessary to add 'data integrity' to Article 14 (6).

9. **COMITOLOGY**

The proposals envisage comitology procedures in several cases where technological decisions for the implementation or the management of the SIS II are required. As it was stated in the VIS opinion for similar reasons, these decisions will have a significant impact on the proper implementation of the principle of purpose and proportionality.

The EDPS advises that decisions with a substantial impact on data protection like for instance access to and introduction of data, exchange of supplementary information, quality of data and compatibility between alerts, technical compliance of national copies, etc. should be made by way of Regulation or Decision, preferably involving a co-decision procedure [1].

[1] See in the same sense, EDPS Opinion on the Visa Information System, Par. 3.12, and EDPS Opinion on the proposal for a Directive on the retention of data processed in connection of the provision of public electronic communication services issued on 26 September 2005, pt.60.

For all other cases with an impact on data protection, the EDPS should be given the possibility to advice on the choices made by these committees.

The EDPS' advisory role should be included in Articles 60 and 61 of the Decision and Article 35 of the Regulation.

In the more specific case of the technical rules for linking alerts (Article 26 of the regulation and Article 46 of the Decision), the need for a different comitology mode (advisory mode for the Decision and regulatory mode for the Regulation) has to be explained.

10. **INTEROPERABILITY**

As the communication of the Commission on the interoperability of emerging EU systems is still lacking, it is difficult to properly evaluate the added value of the foreseen but not yet defined synergies.

In this context, the EDPS would also like to refer to the Declaration of the Council of 25 March 2004 on Combating Terrorism, in which the Commission is asked to present proposals in order to enhance interoperability and synergies between information systems (SIS, VIS and Eurodac). He would also like to refer to the ongoing discussion as to which body could be entrusted with the management of the different large scale systems in the future (see also point 3.8 of this opinion).

The EDPS already stated in his opinion on the Visa Information System that interoperability is a critical and vital requirement for the efficiency of large scale IT systems as the SIS II. It offers the possibility to reduce the overall cost in a consistent manner and to avoid natural redundancies of heterogeneous elements.

— Interoperability can also contribute to the objective of maintaining a high level of security within an area without internal border controls between Member States by implementing the same procedural standard to all the constitutive elements of this policy. However, it is crucial to distinguish between two levels of interoperability:

  — Interoperability between EU Member States is highly desirable; indeed the alert sent by one Member State's authorities have to be interoperable with the ones sent by any other Member State's authorities.

  — Interoperability between systems built for different purposes or with third country systems is far more questionable.

Among the available safeguards used to limit the purpose of the system and prevent 'function creep', the use of different technological standards can contribute to this limitation. Moreover, any form of interaction between two different systems should be thoroughly documented. Interoperability should never lead to a situation where an authority, not entitled to access or use certain data, can obtain this access via another information system. As far as it is possible to discover by the reading of the proposals, it seems for example that an Automatic Fingerprint Identification System (AFIS) will not be present in the first years of the SIS II; only a reference to a future biometric search engine is given. If a scenario where AFIS from other EU systems are used is envisaged, this should be clearly documented with the necessary safeguards required for such synergies.

The EDPS wants to stress again that interoperability of the systems can not be implemented in violation of the purpose limitation principle, and that any proposal in this matter should be submitted to him.

11. **SUMMARY OF CONCLUSIONS**

11.1. **General points**

1. The EDPS welcomes several positive aspects of these proposals, which on some points represent an improvement compared to the present situation. He recognises that provisions on data protection have, generally speaking, been drafted with great care.

2. The EDPS underlines that the new legal regime, however complex should

   — ensure a high level of data protection,

   — be predictable for citizens as well as for authorities sharing data,

   — be consistent in its application to different (first or third pillar) contexts.

3. Moreover, the addition of new elements in the SIS II, increasing its possible impact on the lives of the individuals should be met by more stringent safeguards which are described in the opinion. In particular,

— Access to SIS II data cannot be given to new authorities without the strongest justification. It should also be restricted as much as possible, both in terms of accessible data and authorized persons.

— Interlinking of alerts may never lead, even indirectly, to a change in access rights.

— A non adopted legislation cannot be considered a valid ground for entering data in the SIS II (alerts for the purpose of refusing entry).

— The legal basis for access by authorities in charge of issuing vehicle registration certificates should be reconsidered as it is intended mainly to fight crime.

— The EDPS recognises that the use of biometric data can improve the performance of the system and help the victims of identity theft. However, the impact of this insertion doesn't seem to be sufficiently thought through, and the reliability of these data seems overstated.

11.2. **Specific remarks**

1. The EDPS welcomes the recognition by the Commission that Regulation (EC) No 45/2001 applies to all data processing activities of the Commission in SIS II, as it will contribute to ensure a consistent and homogeneous application of the rules regarding the protection of individuals' fundamental rights and freedoms with regard to the processing of personal data.

2. In order to ensure a strict purpose limitation at national level, the EDPS recommends to introduce in the SIS II proposals (namely Article 21 of the proposed Regulation and Article 40 of the proposed Decision) a provision to the same effect as the current Article 102.4 of the Schengen Convention, limiting the possibility for Member States to provide for use of the data not foreseen in the SIS II texts.

3. Strict conditions should be applied when granting access to SIS II data to any authority:

— Access must be compatible with the general purpose of the SIS II, and consistent with its legal basis.

— The need for access to SIS II data must be demonstrated.

— The use that will be made of data must be defined explicitly and restrictively.

— The conditions of the access must be well defined and restricted. In particular, there should be an up-to-date list of persons entitled to access the SIS II also for Europol and Eurojust.

— The fact that these authorities are granted access to SIS II data can never be a ground for entering or maintaining data in the system if they are not useful for the specific alert they are part of.

— The retention period of the data may not be extended where it is not necessary for the purpose for which the data was entered.

4. In the specific cases of Europol and Eurojust the EDPS urges the Commission to define restrictively the tasks for the performance of which access would be justified. Access by Europol and Eurojust should moreover be restricted to data about individuals whose name already appears in their files. It is also suggested to grant only one access point in the cases of Europol and Eurojust.

5. Concerning the alerts for the purpose of refusing entry, the provisions based on not yet adopted legislation should be either withdrawn or redrafted in a way -based on existing legislation- that allows the individuals to know which measures exactly the authorities can take regarding him/her.

6. The retention periods of the data have been extended without any serious justification being put forward for this. If there is no convincing justification, they should be brought back to their current duration, particularly in the case of alerts for the purpose of discreet surveillance or specific checks.

7. The role of the Commission is described as one of a responsible for operational management. In combination with its major role in the development and maintenance of the system, this should be seen as the role of a *sui generis* controller. It is much more than that of a processor, but also more limited than that of a normal controller, since the Commission has no access to the data processed in the SIS II.

   In application of that role, it should be added in the Article 12 of both proposals that the Commission should regularly propose the implementation of new technologies which represent the state of the art in this field and which will enhance data protection and security levels.

8. Concerning the role of the Member States, clarification is needed as to authorities being controller.

9. Concerning the information of the data subject:

   — In the proposed Regulation, some information should be added to the list: the retention period of the data, the existence of the right to request a review or appeal of the decision to issue an alert, the possibility to obtain assistance from the data protection authority, and the existence of remedies.

     Moreover, as to the moment when this information is provided, an obligation to provide information about the alert in the decision which is the ground for the alert in the first place.

   — In the proposed Decision, Article 50 should be amended in order not to subject the right of information to a request of the data subject.

10. As to the deadlines for answering an access request, the imposition of deadlines in the proposals is welcome. When national legislations also impose deadlines, it should be made clear that the deadlines which are the most favourable to the data subject should be applied.

    Moreover, it would be useful to provide for an obligation of data protection authorities to cooperate actively in the exercise of the right of access.

11. As to the right to remedies, the EDPS suggests dropping the territorial limitation in Article 30 and Article 52.

12. Concerning the powers of the national data protection authorities:

    — in the Regulation: it must be considered that they can exercise, with regard to the SIS II all the competences conferred to them by Article 28 of the Directive 95/46/EC; this should be clarified in the text of the proposed Regulation.

    — As to the proposed Decision: the supervisory authorities should be recognised the same powers as in the Regulation/Directive.

13. Concerning the competences of the EDPS: the EDPS should be able to exercise all his competences under Regulation (EC) No 45/2001, taking into account, however, the limited powers of the Commission with regard to the data themselves.

14. As to coordinated supervision: the proposals also recognise the need to coordinate the supervisory activities of the different authorities involved. The EDPS welcomes the fact that they contain in essence the necessary elements to create the cooperation between the authorities in charge of supervision at national and European level. These provisions (Article 31 of the proposed Regulation and Article 53 of the proposed Decision) could however benefit from some clarifications of the content of that coordination.

15. Articles 10 and 13 of the proposal contain various measures for data security; the inclusion of provisions on systematic (self-)auditing of security measures is welcome.

    — However Article 59 of the proposed Decision and Article 34 of the proposed Regulation, which provide for monitoring and evaluation, should not only concern the aspects of output, cost-effectiveness and quality of services, but also compliance with legal requirements, especially in the field of data protection. These provisions should be amended accordingly.

    — Moreover, in complement to Article 10 (1) (f) or Article 18 of the proposed Decision and Article 17 of the proposed Regulation, it should be added that Member States, Europol and Eurojust should ensure that precise user profiles are available (that should be kept at the disposal of the national supervisory authorities for checks). In addition to these user profiles, a complete list of user identities has to be made and kept permanently up-to-date by Member States. The same applies to the Commission.

    — The lawfulness of the personal data processing operation is based on the strict respect of data security and data integrity. The EDPS should be enabled to monitor not only the security of data, but also their integrity through the analysis of the available logs. It is thus necessary to add 'data integrity' to Article 14 (6).

16. The use of national copies can entail many additional risks. The EDPS is neither convinced of the necessity (considering the available technologies) nor of the added value of the use of national copies. He recommends avoiding or at least seriously limiting the possibility for Member States to use national copies. However, if the national copies are to be developed, a strict purpose limitation principle must be applied to their national use. Similarly, the national copy may never be queried in other ways than the central database.

17. On comitology: decisions with a substantial impact on data protection should be made by way of Regulation or Decision, preferably involving a co-decision procedure. Where the comitology procedure is actually used, the EDPS' advisory role should be included in Articles 60 and 61 of the Decision and Article 35 of the Regulation.

18. Interoperability of the systems can not be implemented in violation of the purpose limitation principle, and any proposal in this matter should be submitted to the EDPS.

Done at Brussels on 19 October 2005.

Peter HUSTINX

European Data Protection Supervisor