The political genesis and legal impact of proposals for the SIS II: what cost for data protection and security in the EU?

Introduction

The Schengen Information System ("SIS") is an EU-wide database of persons and objects whose presence in or entry to the Schengen area[1] of Europe raises issues of public order or security. It became operational on 26 March 1995 and was created as a counterbalance to the suspension of border controls within the Schengen area. All EU member states plus Iceland and Norway[2] have access to the SIS, with the exception of the UK and Ireland who do not currently participate.

Data[12] ("Convention 108"), Directive 95/46/EC[13],

undermines the system's ability to function lawfully as an instrument for executive action.

Investigative action and the merging of purposes

Against this creeping functionality lies a degree of protection. Article 102 of the Schengen convention provides that "Contracting Parties may use the data provided for in Articles 95 to 100 only for the purposes laid down for each type of report referred to in those Articles" [21] unless it is justified by the need to prevent an imminent serious threat to public order and safety, state security, or for the purposes of preventing a serious offence. No such guarantee exists in the SIS II, where links between Article 96 and other alerts are permitted under the Proposed Regulation[22] and Decision[23]. The details of how these links operate are not included in the proposed legislation – the Commission did not want to inflict the details on us : aspects such as the compatibility and links between alerts "cannot be covered exhaustively by the provisions of this Regulation due to their technical nature, level of detail and need for regular update"[24]. The answers are hidden in Council deliberations which clearly anticipate that Article 96 alerts would be linked to all other categories of alert[25]. The Council has provided some illuminating examples of these possible links: "96-98 - pere thesons to be refused entry + witness in an illegal immigration case", "96-99pd - husband convicted criminal to be refused entry + wife suspected terrorist" or indeed "95-99 – husband wanted terrorist and wife suspected accomplice"[26].

Whereas the old SIS created a presumption, that data would only be processed in order to achieve the objective of the specific provision that warranted its entry on the system[27], the Proposed Regulation has a much wider vision whereby the purpose of the SIS II is to "enable competent authorities of the Member States to cooperate by exchanging information for the purposes of controls on persons or objects"[28]. The Commission offers little by way of precision : "data entered on the SIS II pursuant to this Regulation shall only be processed for the purposes and by the competent national authorities defined by the Member States in accordance with this Regulation"[29]. The Commission's explanation of the new functionalities is dangerously circular: "the list of SIS II functionalities contains the existing and the potential new functionalities"[30]. The purpose has become any purposes attributed to competent national authorities for the control of persons - a definition so wide as to create no certainty as to the purpose of the SIS II in practice.

Convention 108, Directive 95/46/EC and Regulation (EC) 45/2001 contain limitations on the purposes for which personal data can be stored. These provisions will apply to the SIS II regardless of the amendments contained in the Draft Regulation and Decision. Despite the attempt by the Commission in its proposed legislation to remove this restriction, certain overarching obligations should continue to apply. Saas points to the possible influence of the ECHR over national courts[31], but a challenge to the interlinking of alerts has yet to be made, as has a challenge before the European Court of Human Rights under Article 8 of the ECHR to the proportionality of refusing a visa or residence permit because of a registration on the SIS.

The President of the Council has acknowledged the transformation of the SIS : "the idea of using the SIS data for other purposes than those initially foreseen, and especially for police information purposes in a broad sense, is now widely agreed upon and even follows from the Council conclusions after the events of 11 September 2001"[32]. This represents the SIS II's development from a hit/no hit system into a much more complex, investigative instrument. The Schengen Joint Supervisory Authority ("Schengen JSA") who together with the European Data Protection Supervisor is is the European body currently responsible for monitoring the SIS and its successors' compliance with data protection

[21] Article 102 (3)

[22] Article 26

[23] Article 46

[24] Recital #19, Proposed Regulation

[25] Note from Presidency on SIS II functions/open issues, Council Doc No 12573/3/04, 30.11.2004, p3

[26] Note from Presidency on SIS II functions/open issues, Council Doc No 12573/3/04, 30.11.2004, p3

[27] Convention 108, Directive 95/46/EC and Regulation (EC) 45/2001

[28] Articles 1(1) Proposed Regulation and Decision

[29] Article 21 (1) Proposed Regulation

[30] Commission Communication to the Council and EU Parliament COM (2003) 771 final Development of the SIS II and possible synergies with a future Visa Information System (VIS), p 15

[31] Saas, Claire "Refus de deliverance de visa fondé sur une inscription au SIS", *Cultures et conflits* www.conflits.org/document.php?id= 917

[32] Note from Presidency to Working Party on SIS Requirements on SIS, Council Doc. 5968/02, 5.2.2002, p2

norms. In its less widely published texts the JSA, has noted this change, not without concern : “the JSA has warned that, as they stand, these proposals would result in a fundamental change to the nature of the system ... the SIS II looks set to become a multi-purpose investigation tool”[33]. This transformation is problematic “it is difficult to see how there can be a proper assessment of the potential implications of the SIS II when its development is to be so flexible that it is unclear what form the system will ultimately take ... [and] must also make it more difficult for those developing the system to take account of the principle of proportionality”[34]. No impact assessment of the SIS II was ever published by the Commission or Council, suggesting that no detailed consideration was given to the implications of the SIS II in terms of data protection or proportionality.

Specified, explicit and legitimate

Under the current provisions of Article 102 the executive action that will be taken pursuant to an alert is to an extent foreseeable to the data subject, but are the ever expanding functionalities lawful? The EDPS has acknowledged that “only a clear definition of purposes will allow a correct assessment of the proportionality and adequacy of the processing of personal data”[35]. Under the SIS II proposals, the interlinking of alerts and the merging purposes of informational assistance, executive action and investigative support jeopardise the data subject’s ability to foresee the consequences of his or her actions, for either free movement or the protection of the right to a private or family life.

Relevant litigation is winding its way through national courts. The European Court of Justice case of Spain v Commission[36] concerns an action brought against Spain with regards to its administra.5(e)-0s7l13.1(refussingvti)7.1sas o -1.(l als)]TJT*012405 Tw[pesionon tke SIS witount h stancSon

judicial, customs, vehicle registration authorities[47] and border agencies in different member states. It would include media both written and oral, and both recorded and unrecorded. It will be used for the exchange of supplementary information[48].

"Supplementary information" is defined as information not stored on the SIS II but connected to SIS II alerts which is *necessary in relation to the action to be taken*[49]. A (presumably new) SIRENE Manual will provide procedural guidance but its precise content will be decided at a later date by the Regulatory Committee on the basis of qualified majority[50]. Unfortunately, its publication is not expected to be imminent either. The content of supplementary information and the way it links to alerts has been omitted from Proposed Regulation, again because it would require details too technical and exhaustive to be included[51].

"Additional data" is defined as data stored in the SIS II and connected to SIS II alerts which is *necessary for allowing the competent authorities to take the appropriate action*[52]. This raises the question of whether additional data is data in addition to the exhaustive provisions of Article 16 of the same Proposed Regulation. The drafting's ambiguity is compounded by the definitions proposed in Article 4 : the difference between information *necessary in relation to the action to be taken*, and information *necessary for allowing the appropriate action to be taken* is moot. Europol, which has access to SIS information under the SIS + 1 proposals, has fallen foul of this nuance: in a 2002 note[53] to the Council it expresses that it could seek additional information from the SIS once a hit had been made. The Council is similarly confused in describing the information to be exchanged after a positive hit : "additional information may be the European Arrest Warrant or the additional information from the SIRENE bureau"[54] In confounding the two terms the Council and Europol point to the problem that the SIS is a poorly defined and very permeable structure, which authorities in different member states can in any event by-pass by contacting each other directly.

The other pillars of the SIS, the Consular Common Instructions ("CCI") and the Common Manual ("CM"), govern the conditions for issuance of a visa. They too were not published in the Official Journal for a number of years[55], and then were done so selectively, with gradual declassification beginning in 2000[56], five years after the system came into operation. As with the exchange of supplementary information under the SIRENE Manual, the conditions under which consular agents are required to contact other central or consular authorities and exchange information remain confidential[57] and unpublished, including the list of nationalities for which this procedure is carried out.

The CCIs provide for "additional documents" to be submitted in support of a visa application. These vary from country to country depending on local migratory risks[58]. They include information exchanged with a view to establishing that the applicant is a bona fide person, and thus subject to fewer checks[59]. There is also a certain amount of informal contact which includes the exchange of information both verbal (likely unrecorded) and written. The existence and exchange of such information is assured by the structure of the SIS, in this case without any corresponding data protection measures.

Guild refers to this volume of information as a "third system of information"[60] where the CCIs provide for no independent control of information circulating between different diplomatic or visa issuing posts and data protection authorities have no explicit powers to intervene.

Under the SIS II proposals this would represent a fourth system of information, the first three being the NI-SIS, the CS-SIS and the "communication infrastructure" provided by the SIRENE bureaux

[47] Proposed Regulation 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, 31.05.2005

[48] Article 4(4) Proposed Decision

[49] Articles 3(1) Proposed Regulation and Decision

[50] Article 61

[51] Recital 19, Proposed Regulation

[52] Articles 3(1) Proposed Regulation and Decision

[53] Note from Europol Council Doc 9323/02, 28.5.2002

[54] Note from Presidency on SIS II functions/Open Issues, Council Doc 12573/3/04, 30.11.2004 p7

[55] Decision of the Executive Committee of 28 April 1999 (SCH/Com-ex (99) 13) OJ L 239 22.9.2000 P. 0317 - 0404

[56] Council Decision 2000/751/EC

[57] Common Consular Instruction Annex 5b OJ C 313/1 and Common Manual Annex OJ C 313/97 16.12.2002.

[58] CCI Part V, #1.4

[59] CCI Part V, #1.4

[60] Guild, Elspeth, Le Visa : instrument de la mise à distance des "indésirables" , *Cultures et conflits* www.conflits.org/document.php?id=933

and SIRENE Manual (and subsequent incarnations). This fourth information system is not defined, not named, not verifiable, in some cases unrecorded. It is "a database that does not speak its name so as not to permit access to this database"[61]. The disparity in consular practice and the existence of hidden data beyond the overtly confidential data of respective Annexes 5b and 14b of the CCI and CM embed this fourth information system in the SIS and SIS II's architecture.

Both hard data, such as that referring to convictions, judgments and administrative decisions, and soft data relating to unconfirmed information, investigations and suspicions, are important in national authorities with the information required to perform their duties. Bearing in mind the wealth of supplementary information available on the SIRENE system as well as on local databases more loosely connected with the SIS, significant amounts of soft data will be available to end users. The Council's own example of spouses suspected of terrorism being included on the SIS with Article 96 alerts is an example of soft data and hard data being mixed.

This presents two major difficulties: the first is that soft data is more difficult to verify and update than hard data, posing significant doubts

reasons for their inclusion on the SIS would not be valid in most of the Schengen states.

The Proposed Decision also provides for the inclusion of European Arrest Warrants ("EWA") on the SIS II[67] and data on criminal prosecutions, both intended and actual, subject to the relevant limitation periods. The plans alarmed the EDPS: "the proposal does not contain all the necessary guarantees for an adequate data protection"[68] in conformity with European norms. The EDPS drew attention to the disparities in national legislation as regards the rights of data subjects in the exchange of information from criminal records[69], indeed common standards in this area have yet to be agreed. The Commission proposed legislation to create a benchmark for the exchange of criminal records in the form of a decision[70] but failed to yield a consensus amongst member states.

Den Boer explains that the complexity of management and decision making in the context of Europe's internal security has required many frameworks situated at numerous levels of governance and administration meaning that "enhanced cooperation in the criminal justice arena may already be a fact" [71]. In spite of divergence in practice and absence of common procedures, the process of exchanging information concerning police, border and criminal activities has already begun, both under the SIS as well as on an ad-hoc basis. The SIS and its

protection appears to be an afterthought in EU policy to expand the SIS, a strategy that carries significant risk.

An important limitation on the effectiveness and fairness of including biometric data in the SIS is technological. At border control and in many police activities, searching for information held on the SIS needs to be an instant process. Including biometric information as an identification system (a one-to-many comparison or "fishing expedition") rather than a verification system (a one-to-one comparison) will slow down the system. The SIS + 1 is as yet incapable of supporting the exchange of fingerprint information, and it is uncertain whether the capacity for an instant response system will exist by the time SIS II is due to be activated. System delay must not result in agencies merely checking the data contained on the NS (which may be out of date) rather than awaiting the results of a search through the NI-SIS and CS-SIS.

Fingerprint data carries with it statistically important limitations. Up to 5% of persons are estimated to have no readable fingerprints or no fingerprints at all. Furthermore, an error rate of 0.5 to 1% for biometric identification systems is normal[77]. In terms of numbers of persons this could affect in any year, up to 1 million may not be able to follow the normal, biometric identifier-led application system, and between 100,000 and 200,000 people a year may be rejected on the basis of an inaccurate identification. The stigmatisation by judicial, police or immigration authorities and nefarious impact on freedom of movement remain possible consequences of undue reliance on fingerprint data.

The Prüm Convention[78] , also known as Schengen III, was signed in Germany on 27 May 2005 by certain member states and is worthy of a mention at this stage. It mirrors the SIS in its design and functions but is directed at Community citizens

protest at international political gatherings. It proposed to enable border checks to be instituted to identify those who are "believed to be intending to enter the country with the aim of disrupting public order and security at the event"[85]. There is a striking absence of any requirement for *serious*, or even *reasonable* grounds for believing that an individual intends to be a violent troublemaker. Grounds for exclusion are therefore subjective, and could include unreasonable or unfounded beliefs. It could suffice for an individual to be suspected of being a member of a political organisation that espouses direct action or protest, or be associated with an individual who is a member. With the purposes of the SIS II and this draft resolution so closely aligned, the Italian proposal bears resemblance to what the Commission might call a proposed SIS II functionality in the making.

Despite the invocation of serious crime and violence to warrant the biometrification and control of data on individuals, impeding free movement on a large scale has mostly been a tool of political control : "the authorities evidently deem controls at internal borders not be an efficient instrument in the fight against serious criminal activities unrelated to political events"[86].

The public policy justification for SIS II exclusions is a case in point. The infrequent use of Article 2 (2) overall reflects that reintroduction of border controls is mainly a symbolic enactment of national sovereignty, subject, in the case of EU citizens and third country nationals with free movement rights, to control by the ECJ. The SIS II is a site of great potency in controlling those within, as well as those seeking to cross the EU's borders.

The provisions for excluding or limiting the movement of persons are not just applicable to third country nationals. Although these cases have not been publicly acknowledged or pursued by the JSA, there are NGOs and lawyers who report that some of their clients, French nationals, "have been registered on the SIS even though this is formally prohibited on the basis of Article 96 which concerns undesireable aliens"[87]. The Proposed Regulation also purports to apply only to third country nationals[88] but it is difficult to ascertain how the new system will be able to exclude its application from EU nationals. This is particularly so in the context of the Spanish proposal that the SIS should have anti terror functions : the London bombings and the Stockwell shooting brought doubt to facile assumptions about nationality and threats to public safety.

The nebulous character of supplementary information disguises the inclusion of personal information regarding EU nationals. Personal information on EU nationals will be held on the SIS and its successors where that individual has sponsored a third country national's visa or residence permit application, is the spouse, child or parent of the third country national, or is travelling in the same group as the applicant. The inclusion of soft data and the linking of alerts will also enable information to be captured very widely. At the time the entry is made on SIS there is no way of knowing that at the time the individual seeks to enter the Schengen area, they have not come to benefit from Community rights. With EU nationals already included in the data to be migrated from the SIS and SIS + 1, and the

[85] Article 2

[86] Groenendijk, Kees (2004), pp150 - 170, p159

[87] Guild, Elspeth "Désaccord aux frontières et politique des visas : les relations entre Schengen et l'Union" *Cultures et conflits* www.conflits.org/document.php?id=927

[88] Article 15 Proposed Regulation

ECJ's decision on the process for finding an infringement of Directive 95/46/EC and the way it relates to a breach of Article 8 ECHR[91] show that an approach should begin with an examination of national law and its compliance with European provisions. If European data protection standards are not met the measures' compliance with the requirements of Article 8 are also called into question.

Adequate, relevant and not excessive

Convention 108, Directive 95/46/EC and Regulation (EC) 45/2001 provide that the information held and exchanged through the SIS must be adequate, relevant and not excessive for the purpose of ensuring public and state security. The leaking of soft data into the SIS has already begun, and is likely to increase with the SIS II. The permeability of additional data, supplementary information and the "fourth information system" suggest that after a hit, authorities would have access to significant amounts of superfluous and unverifiable data. In addition, variations in national practices as regards the reasons for registering an alert suggest that some countries are including information deemed irrelevant by other member states. It is difficult to argue that such information is not excessive, when no EU consensus exists to support its inclusion.

Under the Schengen Convention, personal data should be kept only for the time required to achieve the purposes for which it was supplied, and its retention reviewed no later than three years after the information was included[92]. SIRENE data must also only be kept for such time as required to achieve the purposes for which it was supplied and must be deleted in any event no more than one year after the alert to which it relates has been deleted[93].

The Convention's provisions on the deletion of information have not succeeded in safeguarding the quality of the data held on the SIS. This is partly due to the provisions contained in the SIRENE Manual, which meekly suggest that "As far as is possible, these additional pieces of information should not be kept by the Sirene's once the corresponding alert has been erased"94. The JSA declared this provision in breach of the Schengen Convention95 : the use of data archived for monitoring or technical support purposes to prepare new documents relating to criminal or other matters is likely to constitute a departure from the principle of finality contained in Article 5(2) of Convention 108. In addition, "The existence of a monitoring system after deletion of an alert (...) does not justify archiving documents for an unlimited period of time"[96]. Unless the procedure in the SIRENE Manual or its successor can provide for such limits it will be in breach of this principle.

The German Federal Data Commissioner's Report of 2003/2004[97] on German N-SIS data reveals a number of shortcomings. In many cases, there was no record of a review as mandated by Article 112 to determine the need for continued storage of personal data. It was often impossible to determine how long an alert had been in effect due to a lack of documentation. In some cases, alerts had remained active for up to nine years. In nearly 50% of cases, the time limit for the alert in the SIS was linked to a permanent national ban on entry, and therefore not issued for a limited period of time. Lastly, deleting the alert in the SIS did not always entail deleting the records on which it was based.

Individuals currently have limited rights to access information held on them in the SIS[98]. They have a right to correct such information or to have it deleted if it is held unlawfully, or to seek compensation. They can also ask a national data protection authority to check the information held on them in the SIS[99]. These provisions are mirrored by the Proposed Regulation and Directive. Under the Proposed Regulation individuals would gain the right to review or appeal a decision to issue and alert[100] but the modalities of review or appeal are not expressed,

---

[91] Joined Cases C-465/00, C-138/01 and C-109/01, Rechnungshof, Osterreichischer Rundfunk and others, Judgment of the Court, 20.5.2003 (1)

[92] Article 112 Schengen Convention. Debate as to whether Article 113 applied instead (where the maximium period of retention was 10 years) was convincingly settled by the opinion of the JSA Opinion Concerning the relation between Articles 112 and 113 Schengen Convention SCHACH 2510/1/02 REV1, 7.10.2002

[93] Article 112A Schengen Convention

[94] SIRENE Manual # 2.1.3(b).

[95] Recommendation from the Schengen JSA SCHAC 2505/99 LIMITE, 11.10.1999

[96] Recommendation from the Schengen JSA SCHAC 2505/99 LIMITE, 11.10.1999 p3

[97] German Federal Data Commissioner Report 2003 2004, www.bfd.bund.de/information/tb04_engl.pdf, pp22-23

[98] Article 109 Schengen Convention

[99] Articles 110 and 111 Schengen Convention

[100] Article 15(3) Proposed Regulation

nor is any remedy, penalty or requirement as to suspensive effects over removal measures.

Data subjects are currently prevented from accessing information held on them in the SIS if it is indispensable for the performance of an action connected to the alert or to protect the rights and freedoms of others. This restriction is lifted in the Proposed Regulation. Regulation 46/95/EC[101] does contain loose grounds for restricting access (in the case of public security or the protection of rights and freedoms of others) which should nonetheless apply. The current right to ask a supervisory authority to verify data in cases where individuals have been refused access is absent in the Proposed Regulation. This blunts the teeth of the EDPS. The interlinking of alerts is also pertinent to data subject access, as it renders the application of a 'blue pencil' test, whereby restricted and available data are severed, problematic.

The right to be informed when an alert is issued in a person's regard remains absent in the proposals. The right to compensation for illegal or incorrect entries is delegated to national law, where judicial systems may not be accessible to those denied entry to the EU. The applicant's need for territorial presence to access the courts is necessary for actions in respect of the SIS II's immigration provisions under the Proposed Regulation[102], but not for actions under the Proposed Decision. The discrepancy in territorial provisions may be resolved by the final drafts but unless they are settled in the applicant's favour, the data subject's access to justice will be inhibited.

A 2002 French case[103], unreported, concerns the exercise of national data supervisory authorities' powers to access and verify information on the SIS. In this case, Mr Moon and his wife were refused entry by France on the basis of an information input by another member state. Mr Moon, not permitted to verify the information himself, asked the Commission nationale de l'informatique et des libertés ("CNIL") to do so on his behalf. In its response the CNIL confined itself to confirming the information had been verified. The court held that the fundamental rights of access and rectification were deprived of practical value by the curtness of the CNIL's answer, and ordered the CNIL and the Minister of

[101] Article 13

[102] Article 31(1)

[103] Moon, Re (Unreported, November 6, 2002) (CE (F)) Conseil D'Etat (Assemblée), case comment by Roger Errera, *Public Law* 2003, SPR, 187-190imsehr0.0004 Tc0.05.007 136.8((uyr4 Tm-0.4182 Tc0.5503In thioate.)[(itmmu)6(annTwt8.1)4

and overall, police, border guards and judicial bodies are already authorised to access and amend all data processed under articles 95 - 100. For the most part, immigration authorities within the country plan to gain access to Article 96 alerts only.

In reality, the existence of these 125,000 access terminals and the increasing number of bodies and member states permitted to access them makes compliance with the Schengen Convention's confidentiality requirements difficult. In 1998 a written question by a Greek MEP revealed that SIS information had been leaked by Belgian police to local gangs.[108] A 1999 report by Justice on European Databases described procedures in the Netherlands, where the rooms housing the Interpol computer terminals and the SIRENE terminals are "adjacent, separated only by a smoked glass partition and open door. SIS operators work a 24 hour shift system, whereas those on Interpol terminals work regular office hours; SIS personnel handle any important Interpol business during off-hours"[109]. A comprehensive account of practices in different members states would provide much needed information for an EU wide assessment of the operational risks and processes..

UK and Ireland's access to Article 96 alerts

UK and Ireland participate selectively in the Schengen acquis[110] including SIS provisions, save those concerning Article 96 alerts. Cross border police activities, however, are within UK participation.[111] It has not been conclusively decided which UK agencies will access the information and to what extent the UK will effectively continue to exclude application of Article 96 of the Schengen Convention. This ring-fencing of Article 96 alerts from access by the UK and Ireland goes against the obligation under Article 92(2) of the Schengen Convention for the different N-SIS to be identical in content. Article 94 limitations on the use of data are removed in the SIS proposal and indications on how the interlinking of alerts will comply with limitations on access have not yet surfaced in the morass of documents currently listed on EU registers.

The JSA rejected the UK solution of allowing all information to be accessed by a few select individuals in the UK N-SIS, being in breach of the Schengen Convention. The Dutch solution to place a filter at the C-SIS level to prevent the transmission of Article 96 information to the UK and Ireland whilst providing a facility to check for double alerts was accepted[112]. The JSA expressed that any option must also comply with the data protection principle enshrined in Article 94, but the proposals mean the UK and Ireland's future participation in the SIS risks contamination by Article 96 data and alerts.

Exchange of information with third parties

The Council introduced Decision 2004/496/EC[113] requiring air carriers flying to, from or over the United States to provide United States Department of Homeland Security, Bureau of Customs and Border Protection with electronic access to information held on passengers. This is a "pull" system, with US authorities entitled to request and receive information from carriers. To comply with Directive 95/46/EC the Commission adopted Decision 2004/535/EC in which it decided that US authorities provided adequate data protection measures. This cleared the way, or so it thought, for the wholesale transfer of passenger data contained on carriers' information systems to US customs and internal security agencies. These Decisions have been controversial. The European Parliament submitted conclusions to the ECJ[114] to annul the agreement and the Decisions and the EDPS has now been granted permission[115] to support the European Parliament in its action.

The Parliament argues that because the agreement entails the transfer of sensitive data in breach of Article 8 of Directive 95/46/EC, an amendment of that Directive is implied. The co-decision of the European Parliament should therefore have been obtained and the decisions were therefore ultra-vires. Furthermore, the agreement constitutes an unjustifiable

[108] Written question No. 19/98 by Nikitas KAKLAMANIS to the Commission. Official Journal C 196 , 22/06/1998 P. 0107

[109] Submission by Justice to the House of Lords European Communities Committee (Sub Committee F) on European Databases, April 1999, p11

[110] as referred to in Article 1(2) of Council Decision 1999/435/EC

[111] Council Decision 2000/365/EC

[112] Note from the Chairman of the JSA to the Chairman of the Article 36 Committee, SCHAC 2502/2/02 REV 2, 11.3.2002, p6

[113] Council Decision 2004/496/EC on the conclusion of an Agreement between the European Community and the USA on the processing and transfer of PNR data by Air Carriers to the US Department of Homeland Security Bureau of Customs and Border Protectiority comp4638d7e conclusion

interference with private life and is thus incompatible with Article 8 of the ECHR. The breach arises through the transfer of large volumes of information to a third party without the consent of the persons concerned, and without providing a way of controlling the consequences of the transfer[116]. On account of the excessive amounts of data processed, and because the US authorities hold the data for too long, the measures are not proportional. Lastly, the hurried implementation of the decisions, which failed to await an opinion by the ECJ requested by the Parliament, is in breach of the Community law principle of cooperation in good faith. This case will test the effectiveness of the EDPS and the European Parliament, and represents a real challenge to the political imbalance in community procedures..

The EU has now agreed similar measures with the Canadian authorities albeit under a "push" system. Here, the EDPS approved[117] the main elements of the agreement. In this case, the measures provide for more limited data to be transferred which does not include of open-ended categories of personal and potentially sensitive information. Despite its developed system of data protection, Canada cannot ensure compliance with Directive 95/46/EC in granting full protection to EU citizens, and the EDPS calls for amendment of the agreement in that respect.

"The absence of such a mandate is particularly striking (...) The only provision that enables Eurojust access to SIS data appears to be an unpublished non-legally binding declaration annexed to the Eurojust Decision (which we have asked to see but have never received)."[126] Furthermore, whilst Europol is permitted to request and receive information from third states and organisations, the Europol database cannot be connected to any other system directly. The Proposed Decision states that Europol may not connect to or download or otherwise copy any part of the SIS II[127]. These provisions are a fig-leaf if Europol can access NS information, which could include copies of SIS II information entered on the system by different member states, directly.

impossible to make, but the Committee found that the EDPS lacked the facilities to properly monitor data protection, and was critical of Article 3 of the draft regulation, which provides for links to "other" (undefined) applications.

The SIS II will interconnect with the VIS, Europol Information System and Customs Information System. It will be accessed by vehicle registration authorities, as well as police, border and judicial bodies. It will be linked with third states and organisations. It will be linked to shared data platforms such as the Communication and Information Resource Centre Administrator (CIRCA). This integration of databases is leading to a widening of police powers[135] and points to a danger of interoperability - that it creates the possibility for an authority, denied access to certain data, to obtain access to it via a different information system. The Commission estimates that the VIS alone will handle approximately 20 million visa applications per year. Information relating to these applications can be stored for up to 5 years. This represents vast data, and data

exchange regulated through measures to amend the SIRENE Manual, CCIs and CM approved by the European Parliament. There should be acknowledgement of the effects of the measures on both EU nationals and persons with Community rights. The EDPS should be granted powers to access, verify, amend and report on SIS II data in a manner that is transparent and available to persons in the EU or excluded from its territory.

With the use and transfer of supplementary information and that contained on the fourth information system, the SIS reaches into the borders of Europe to be used against EU and third country nationals alike, in investigations at local level by national agencies in the course of their normal police and judicial responsibilities.

The expansive application of the public policy basis for refusing entry to the EU represents a dangerous mutation in the subjective notion of a threat to security.

Bibliography

Amann V Switzerland (Application no. 27798/95), 16.2.2000

"I/A" Item note from General Secretariat on C.SIS installation and exploitation budged for 2006 Council Doc 8997/05 SIRIS 44 COMIX 326 OC 287, 27.05.2005

Baldwin-Edwards, Martin (1997) The emerging European immigration regime: some reflections

Council Decision 2004/496/EC on the conclusion of an Agreement between the European Community and the USA on the processing and transfer of PNR data by Air Carriers to the US Department of Homeland Security Bureau of Customs and Border Protection ,OJ L 183 of 20.5.2004, P83)

Council Decision 2004/512/EC OJ L 213, 15.6.2004

Council Decision 2005/211/JHA OJ L 068 , 15/03/2005 P. 0044 – 0048

Council Regulation (EC) 871/2004 OJ L 162 , 30/04/2004 P. 0029 - 0031

Council Regulation (EC) No 2424/2001 OJ L 328 , 13/12/2001 P. 0004 - 0006

Decision of the Executive Committee of 28 April 1999 on the definitive versions of the Common Manual and the Common Consular Instructions (SCH/Com-ex (99) 13) OJ L 239 22.9.2000 P. 0317 - 0404

Den Boer, Monica (2004) *Plural Governance and EU Internal Security: Chances and Limitations of Enhanced Cooperation in the Area of Freedom, Security and Justice,* Paper for ARENA, Oslo, 25.5.2004

Directive 64/221/EC OJ 056, 04.04.1964 P. 0850 - 0857

Directive 68/360/EC OJ L 257 , 19.10.1968 P. 0013 - 0016

Directive 95/46/EC OJ L 281 21.11.1995 P 0031 - 0050

Directive 2004/38/EC OJ L 229 , 29.06.2004 P. 35 – 48

Draft Council Regulation on standards for security features and biometrics on passports and travel documents, Council Doc 15139/04 LIMITE VISA 208 COMIX 714, 23.11.2004

Draft Council Resolution on security at European Council meetings and other comparable events, 30.06.2003, Council Doc. 10965/03 ENFOPOL 63 COMIX 417

German Federal Data Protection Commissioner, Annual Report 2003/2004 of the Federal Commissioner for Data Protection, www.bfd.bund.de/information/tb04_engl.pdf

Groenendijk, Kees (2004) "Reinstatement of controls at the internal borders of Europe : Why and against whom?" in *European Law Journal*, Vol.10 No. 2, March 2004, pp150 - 170

Guild, Elspeth "Désaccord aux frontières et politique des visas : les relations entre Schengen et l'Union" *Cultures et conflits* www.conflits.org/document.php?id=927

Guild, Elspeth, "Le Visa : instrument de la mise à distance des "indésirables" , *Cultures et conflits* www.conflits.org/document.php?id=933

Guiraudon, Virginie, (2001) *The EU "garbage can": Accounting for policy developments in the immigration domain,* .Paper presented at the 2001 conference of the European Community Studies Association in the panel "Immigration and the Problems of Incomplete European Integration," Madison Wisconsin, 29 May-1 June 2001, http://www.eustudies.org/GuiraudonPaper.do

Hustinx, Peter J. (2004) European Data Protection Supervisor, Speech given at Scientific Conference on New Ideas and Trends in the Field of Third Pillar and Law Enforcement Data Protection, Budapest ,1.12.2004

Joined Cases C-465/00, C-138/01 and C-109/01, Rechnungshof, Osterreichischer Rundfunk and others, Judgment of the Court, 20.5.2003 (1)

Joint Supervisory Opinion on the development of the SIS II, 19.5.2004

JSA information leaflet "Your Rights and the SIS" (undated)

JSA Opinion on the development of SIS II, SCHAC 2504/04

January 2002 to 31 December 2003, Council Doc 7915/04 LIMITED SIRIS 47 COMIX 226, 2.4.2004

Note from Netherlands, German, Austrian and Belgian delegations on SIRPIT (Sirene Picture Transfer) – SIRENE Procedure, Council Doc. 9450/02, LIMITE SIRENE 41 COMIX 374, 30.5.2002

Note from Presidency on SIS Database Statistics, Doc No 8621/05 SIS-TECH 38 SIRIS 38 COMIX 285, 2.6.2005

Note from Presidency on SIS II functions/open issues, Council Doc No 12573/3/04, REV3 LIMITE SIRIS 94 COMIX 566, 30.11.2004

Note from Presidency on Mandate for a technical analysis concerning the implementation of Article 1(9) of Decision 2005/211/JHA - Access to the SIS for Europol, 8874/05 SIRIS 42 SIS-TECH 47 COMIX 310

Note from Presidency on Assessment of the state of the SIS II project Council Doc 9672/05 LIMITE SIRIS 56 COMIX 366

Note from Presidency on Comments on the Commission's progress report for SIS, Council Doc 8506/05 LIMITE SIS-TECH 36 COMIX 272, 27.4.2005

Note from Presidency on JHA Council Declaration: follow up, Council Doc 11330/05

Note from Presidency on Parameters, procedures and time schedule for decision on the strategic management of SIS II, Council Doc 12888/04 LIMITE JAI 355 SIRIS 98VISA 176 COMIX 582, 4.10.2004

Note from Presidency on SIS Requirements, Council Doc. 5968/02, 5.2.2002

Note from the Chairman of the JSA to the Chairman of the Article 36 Committee, SCHAC 2502/2/02 REV 2, 11.3.2002

Opinion of the European Data Protection Supervisor on the Proposal for a Regulation of the European Parliament and Council concerning the

Thym, Daniel: The Schengen law : a challenge for accountability in the European Union, *European Law Journal* Vol. 8 No. 2, June 2002, pp218 – 245, p242

Van Buuren, Jelle "Les tentacules du système Schengen" *Le Monde Diplomatique*, March 2003 http://monde-