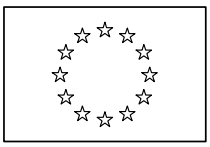

COMMISSION OF THE EUROPEAN COMMUNITIES

Brussels, 24.11.2005
COM(2005) 597 final

COMMUNICATION FROM THE COMMISSION TO THE COUNCIL AND THE EUROPEAN PARLIAMENT

on improved effectiveness, enhanced interoperability and synergies among European databases in the area of Justice and Home Affairs

COMMUNICATION FROM THE COMMISSION TO THE COUNCIL AND THE EUROPEAN PARLIAMENT

on improved effectiveness, enhanced interoperability and synergies among European databases in the area of Justice and Home Affairs

1. CONTEXT

On several occasions, and in the context of combating terrorism and improving internal security, both the European Council and the Council of the European Union have called upon the Commission to submit proposals for improved effectiveness, enhanced interoperability and synergy among European databases (Declaration of 25 March 2004 on combating terrorism[1], the Hague Programme[2], Council Declaration of 13 July 2005 following the London bombings).

The European Council and the Council have also repeatedly underlined the importance of using biometrics in databases and travel documents to enhance the level of security of the European Union.

2. DEFINITIONS AND PURPOSE OF THIS COMMUNICATION

2.1. Purpose of this Communication

The context in which the request to draft this Communication was made – combating terrorism and crime –indicates that its purpose goes further than substantially improving technical interoperability and synergy of information technology (IT) systems in the area of Justice and Home Affairs.

The purpose of this Communication is to highlight how, beyond their present purposes, these systems can more effectively support the policies linked to the free movement of persons and serve the objective of combating terrorism and serious crime.

A delicate balance between the pursuit of these objectives and the protection of fundamental rights (notably the protection of personal data), as embodied in the European Convention of Human Rights and in the Charter of Fundamental Rights of the European Union, must be found. It must also be borne in mind that IT systems can serve to protect and amplify the fundamental rights of the individual.

This Communication should trigger in-depth debate on the long-term shape and architecture of IT systems. In identifying possible scenarios, including those that may be far-reaching in ambition and impact, this Communication does not prejudge the results of an in-depth debate by passing judgment on if, when and under which

---

1 Council of the European Union 7906/04 Declaration on combating terrorism 29 March 2004

2 The Hague Programme: strengthening freedom, security and justice in the European Union, 10 May 2005

conditions these scenarios should be implemented. Also, given its political and strategic approach, it does not address or assess, in detail, the legal[3], technical, organisational or societal impact of possible solutions. Prior to any legislative action, in-depth impact assessments will need to be carried out, especially with regard to proportionality. Such assessments should also address the impact on other existing or planned means of cooperation between authorities responsible for internal security (e.g. via Europol).

This Communication begins with a short description of the current situation of existing and future pan-European IT systems and the gaps identified in the pursuit of their current objectives. Next, scenarios for using these systems in a more efficient manner and for creating possible future systems will be presented. Finally, consideration as to whether the technical and operational possibilities are proportionate and compatible with the need to protect the rights of the individual is explored.

This Communication does not propose measures for further interoperability and synergy at national level. Although measures adopted at European level are likely to have an effect on national systems, it is up to each Member State to analyse how national systems could better interact.

2.2. Concepts

Before going into further detail, the following concepts should be clarified.

"Interoperability" is the "ability of IT systems and of the business processes they support to exchange data and to enable the sharing of information and knowledge"[4]. "Interoperability" is a technical rather than a legal or political concept. This is disconnected from the question of whether the data exchange is legally or politically possible or required[5].

"Connectivity" is a generic term for connecting devices in order to transfer data.

"Synergy" encompasses technical, economical and organisational elements. Technically, "synergy" means a mutually advantageous conjunction of several elements. Economically, it means an increase in the value of assets or an economy of scale. Organisationally, "synergy" means combining previously distinct resources or streamlining the existing organisation so as to increase efficiency.

The *"principle of availability"* means that authorities responsible for internal security in one Member State or Europol officials who need information to perform their duties should obtain it from another Member State if it is accessible there.

---

3 Including the scope of participation of countries that do not (fully) participate in the "Schengen acquis".

4 European Interoperability Framework for Pan-European eGovernment Services, Office of Official Publications of the European Communities, 2004, point 1.1.2.

5 The details of how organisations agree to technically interact with each other when exchanging data is usually laid down in an interoperability framework that can be defined as a set of standards and guidelines, see European Interoperability Framework for Pan-European eGovernment Services, Office of Official Publications of the European Communities, 2004, point 1.1.2.

3. STATUS AND PURPOSE OF EXISTING AND FUTURE IT SYSTEMS

This Communication focuses on SIS II, VIS and EURODAC as the systems that have been particularly highlighted by the European Council and by the Council in their mandate. Each system pursues a specific objective; the personal data they process are not necessarily the same as they are limited to those that are relevant for the objective of a specific system. Equally, the authorities empowered to access personal data are not always the same.

3.1. SIS II

The second generation Schengen Information System (SIS II) will make border crossing easier in the enlarged European Union without compromising security. It allows authorities in the Member States to cooperate, by exchanging information, in order to establish an area without internal border controls. The information obtained will be used for controls of persons at external borders or on national territory and for the issuance of visas and residence permits, as well as for police and judicial cooperation in criminal matters[6].

3.2. VIS

The Visa Information System (VIS), will benefit bona fide travellers by improving visa issuing procedures. It will improve administration of the common visa policy and consular cooperation in order to: prevent threats to internal security and 'visa shopping'; facilitate the fight against fraud; assist in the identification and return of illegal immigrants; and facilitate application of the Dublin II Regulation[7].

On 7 March 2005, the Council concluded that authorities responsible for internal security should be given access to VIS. The Commission will table a proposal allowing both Europol and the authorities responsible for internal security to access the VIS for clearly defined purposes.

3.3. EURODAC

The purpose of EURODAC is to assist in determining which Member State is responsible pursuant to the Dublin II Regulation and to facilitate its application. EURODAC is essential in ensuring the efficiency of the European Asylum System.

4. IDENTIFIED SHORTCOMINGS

Although SIS II, VIS and EURODAC are the focus of this Communication, other issues related to combating terrorism and crime are also discussed.

---

6 The conditions governing the processing of personal data will be defined in the legal instruments regulating SIS II.

7 Council Regulation (EC) 343/2003 of 18 February 2003 establishing the criteria and mechanisms for determining the Member State responsible for examining an asylum application lodged in one of the Member States by a third-country national, 0.J. L50 of 25.2.2003

4.1. Under-exploitation of existing systems

Currently, all the existing systems are not fully exploited. This relates, e.g. to some categories of alerts in the SIS, such as alerts issued for discreet surveillance or specific checks used in a limited and heterogeneous way. Increased and more consistent use of these alerts could enhance the fight against terrorism. Finally, besides the data processed in common systems, many Member States maintain separate lists for the same purpose, for example for refusal of entry, resulting in duplication of effort for many Member States.

The EURODAC Regulation is also under-exploited. Although the EURODAC Regulation obliges Member States to take fingerprints of all persons aged over 14 who cross their borders irregularly and cannot be turned back, the quantity of such data sent to EURODAC is a surprisingly low fraction of the total migratory flow.

4.2. Limitations to alphanumeric searches

An alphanumeric search cannot be successful unless the information is fairly accurate. As regards persons, the probability of not obtaining correct results increases with the size of the database. The more names there are in the database, the harder it is to find a person and the more likely it is to identify a person wrongly. Erroneous information (e.g. a name or birth date from a forged document, or different transliterations of the same name) gives false results. In addition, an alphanumerical search with data that are not unique will become less accurate the more data are stored in the database, resulting in long "hit" lists, which must then be verified through a labour-intensive process that is sometimes impossible to perform in a border-control environment.

4.3. No benefits for frequent bona fide travellers

Of all those applying for a Schengen visa, 20% are estimated to be regular travellers, i.e. applying for repeat visas. For these travellers, there is little scope for speeding up visa processing times. If travel documents are lost or stolen, bona fide travellers must complete a complicated process to acquire new travel documents.

4.4. Identification of illegal immigrants is difficult

Many apprehended illegal immigrants have no identification documents with them or use counterfeit or falsified documentation. In such cases, the identification process is time-consuming and expensive. If travel documents have been destroyed, authorities currently do not have a system to check identity.

4.5. Inefficiencies in the application of the Dublin II Regulation

This Regulation defines the criteria for determining the State responsible for examining asylum applications. A basic criterion is whether a Member State has issued or extended a visa to the asylum seeker. At present, Member States do not have efficient means to check whether an asylum applicant has had a visa issued by another Member State, verify the identity of the person, and determine the validity of the visa.

4.6. No possibility to use asylum, immigration and visa data for internal security purposes

In relation to the objective of combating terrorism and crime, the Council now identifies the absence of access by internal security authorities to VIS data as a shortcoming. The same could also be said for all SIS II immigration and EURODAC data. This is now considered by the law enforcement community to be a serious gap in the identification of suspected perpetrators of a serious crime.

4.7. Not all categories of third-country nationals are checked

VIS currently only deals with third country nationals, under visa obligation. The control of the identity or the legality of the entry of other categories of third-country nationals who frequently cross borders, e.g. holders of a long-stay visa or a resident permit, or third-country nationals not subject to a visa requirement could also be more efficient. This has been identified as a shortcoming by the internal security and intelligence communities.

4.8. Incomplete monitoring of entry and exit of third country nationals

Although the VIS will allow the checking of visa application history and whether the person presenting the visa at the border is the one to whom it has been issued, VIS does not track entries of third-country national visa holders; nor does it track whether third-country nationals leave before the end of their right to stay expires. In other words, neither VIS (nor SIS II, for that matter), can identify persons illegally remaining in the EU.

4.9. Lack of biometric identification tools

A basic requirement for authorities responsible for combating crime and terrorism is to identify persons for whom only biometric information is available, e.g. a photo, a fingerprint or a DNA code. Automated Fingerprint Identification System (AFIS) and DNA databases allow such identification. As such databases now exist in most Member States, the Commission services are currently working on a proposal to interlink national DNA databases. The Commission also intends to present a legal instrument as regards fingerprints next year. As currently developed, SIS II will only allow for the introduction of an alert if at least basic alphanumeric information can be entered in the system. The fact that the Treaty of Prüm, signed by seven Member States on 27 May 2005, will introduce an exchange of fingerprint and DNA data on a bilateral basis, pending the adoption of such an instrument at the European level, highlights this gap.

4.10. No registration of EU citizens at European level

The identification of EU citizens on the basis of travel and identity documents will soon be improved by the introduction of biometric identifiers. However, although most Member States will have a central repository of issued documents and biometric identifiers linked to a certain identity, a query of that central repository only allows a check as to whether in that same Member State a document has been previously issued to the same person under another name. In addition, it is currently

not possible to launch a query on a person who is, say, wanted for a terrorist crime on the basis of whether this person has ever been issued with a travel or ID document.

This has also been identified as a gap in the fight against identity theft which causes increasing concern among authorities responsible for internal security and substantially damages the European economy.

4.11. Identification of disaster victims and unidentified bodies

There is no comprehensive database which would allow for the identification of disaster victims and unidentified bodies. The possibility to make use of an Interpol database for this purpose has been discussed in the Council. However, such a database will not be able to cover all cases.

5. FURTHER POSSIBLE DEVELOPMENTS

5.1. Better use of existing systems

A more efficient use of current systems can first and foremost be achieved by enhanced use of the possibilities that exist: better quality control of data in-put, more coherence as regards input of data categories and improved user-friendliness. In this respect, wider and more direct consultation of Member States and exchange of best practices would be useful. Although this consultation should be achieved primarily in existing working groups and committees, regular user conferences could help. This additional consultation could identify where there is need for improvement and results could then be fed into the legislative process and/or daily practice.

In addition, more consistent introduction and use of certain data (for example SIS II alerts on persons who are likely to commit serious criminal offences and EURODAC data on irregular border-crossers, etc.) should be made by Member States.

5.2. Further development of existing systems and planned systems

5.2.1. Biometric searches in SIS II

Identifying persons in databases with millions of entries has been solved in EURODAC and will be addressed in the VIS by using biometric searches, allowing unprecedented accuracy. The proposals for the SIS II legal instruments allow the processing of biometric information (photographs and fingerprints). However, as the SIS II is being developed today, biometrics will only be used to confirm the identification of the wanted person (wanted persons meaning "persons for whom an alert has been issued", including persons who should be refused entry) based on an alphanumerical search.

When available, biometric searches would allow more accurate identification of wanted persons. However, SIS II would only store biometric information that could be legally linked to an alert in SIS II.

5.2.2. More comprehensive access to VIS and SIS II by asylum and immigration authorities

Legislative proposals foresee access to VIS and SIS II by asylum authorities. On the one hand, VIS and SIS II will contain data which may indicate that one of the criteria for determining the Member State responsible is fulfilled: the issuance of a visa or an illegal stay in a Member State. On the other hand, VIS and SIS II may contain data that completes the assessment of an asylum application: visa data can help to assess the credibility of an asylum claim and SIS II data can indicate if the asylum seeker constitutes a threat to public order or national security. A check in EURODAC, SIS II and VIS would allow asylum authorities to check the data simultaneously in the three systems.

Access to VIS and certain biometric SIS II data would have a significant impact on the fight against illegal migration. Undocumented illegal migrants would be easily identified. This would help in checking whether persons entered lawfully and also in documenting persons for removal.

5.2.3. Access by authorities responsible for internal security

As regards the VIS, a draft legal instrument extending the access of authorities responsible for internal security for the purposes of the prevention, detection and investigation of terrorist offences is being presented by the Commission.

As regards SIS II data related to refusal of entry, an extension of access for purposes linked to the prevention, detection or investigation of a crime should be envisaged for authorities responsible for internal security. This should be articulated in the framework of other existing possibilities to process data related to persons who represent a threat to security. Specific issues such as reciprocity with Member States that do not fully participate in the policies linked to the free movement of persons would also have to be addressed.

As regards EURODAC, the only information available to identify a person may be the biometric information contained in EURODAC if the person suspected to have committed a crime or an act of terrorism has been registered as an asylum seeker but is not in any other database or is only registered with alphanumerical, but incorrect data (for example if that person has given a wrong identity or used forged documents). Authorities responsible for internal security could thus have access to EURODAC in well-defined cases, when there is a substantiated suspicion that the perpetrator of a serious crime has applied for asylum. This access should not be direct but through the authorities responsible for EURODAC.

Access to these systems could also contribute to the identification of disaster victims and unidentified bodies.

5.3. Long-term scenarios and further developments

5.3.1. Creation of a European criminal Automated Fingerprints Identification System (AFIS)

Beyond the proposal already mentioned on the comparison of DNA profiles, a European AFIS could be created, combining all fingerprint data currently only

available in national criminal AFIS systems. This AFIS could be either a centralised European AFIS or a de-centralised solution (linking existing AFISes). It would be used for police investigation purposes and would go beyond the hit/no-hit biometric search described above for SIS II.

It would again contribute to the identification of disaster victims and unidentified bodies.

5.3.2. Creation of an entry-exit system and introduction of a border-crossing facilitation scheme for frequent border crossers

The main purposes of an entry-exit system are to ensure that people arriving and departing are examined and to gather information on their immigration and residence status. When entering and leaving the European Union, third-country nationals would register, using biometric identifiers. However, the extension of such an entry-exit system to EU citizens could not be envisaged as this would be incompatible with the principle of free movement.

The question may arise as to whether such a solution is feasible, given the high volume of daily travellers crossing the borders of the European Union. In order to reduce the checks, a programme could be introduced for known bona fide travellers (i.e. commuters) to facilitate and automate the border-crossing process. A similar programme is running between the United States, Canada and Mexico, where bona fide travellers, after a particularly careful background check, are issued a "trusted traveller card" allowing border–crossings in an almost fully-automated fashion. Exit registration could be via a self-registration procedure; the incentive to do so being that if no exit has been registered, future entry would not be granted or would be granted only after undergoing a specific procedure.

Although an entry-exit system would enable much more efficient and effective border controls, it would be a huge organisational step and might therefore be risky and costly to implement. However, the situation could be reassessed when the VIS is operational.

In any case, impact assessments or similar measures will have to be carried out in order to assess the proportionality of this and other scenarios presented.

5.3.3. European register(s) for travel documents and identity cards

Most Member States will create their own databases of issued travel documents and identity cards, including biometric identifiers enrolled at application. The effectiveness of these databases could be significantly enhanced if a register of indexes is established at European level. Alternatively, national databases could be interlinked. Whatever the adopted solution, these registers could contain only a very limited set of data (document number and biometrics) but would allow a check on the authenticity of every travel or ID document issued in a Member State and to determine, using biometric information, the identity of any person to whom a travel or ID document was issued.

This approach could also contribute to the identification of disaster victims and unidentified bodies.

5.4. Architectural and organisational changes

Without going into a detailed analysis of technical and organisational changes required to implement the above-mentioned scenarios, the development of a service-oriented architecture of European IT systems would help maximise synergies and would contain investments at a realistic level. A service-oriented architecture is a way of sharing functions in a flexible and cost-efficient way without merging existing systems. In concrete terms, one example would be to use the highly-performing future AFIS part of the VIS to deliver AFIS–related services (i.e. a biometric search for other applications, such as EURODAC or, possibly, a biometric passport register). Data storage and data flow could still be strictly separated.

On the organisational level, it goes without saying that bringing the daily management (i.e. not necessarily the strategic or political management) of these systems together in a single organisation would also bring about significant synergy effects. Managing applications in a single organisational environment is therefore an option that should be examined as a long-term goal. In relation to the objectives of the proposed Freedom programme[8], the question of entrusting tasks related to the management of large-scale IT systems (EURODAC, SIS II, VIS) to the External Border Agency at a later stage is one of the alternatives to be explored.

6. COMPATIBILITY OF POSSIBLE MEASURES WITH HUMAN RIGHTS INCLUDING DATA PROTECTION

As regards the better identification of wanted persons whilst the storage of personal data in criminal databases is justified due to past and real or suspected behaviour of the individual (which must be substantiated), this is not the case for EURODAC or VIS. Neither the claiming of asylum nor a visa application indicates in any way that a hitherto innocent individual will commit a criminal or terrorist act.

The proportionality principle therefore requires that these databases be queried only for the purpose of preventing and investigating serious criminal or terrorist crimes or identifying the perpetrator of a suspected criminal or terrorist act once there is an overriding public security concern, i.e. if the act committed by the criminal or terrorist to be identified is so reprehensible that it justifies querying a database that registers persons with a clean criminal record. The threshold for authorities responsible for internal security to query EURODAC, SIS II immigration data or VIS must therefore always be significantly higher than the threshold for querying criminal databases. In order to ensure full respect for the rights as laid down in Articles 6, 7, 8, 48 and 49 of the Charter of Fundamental Rights of the European Union, the scope for access should thus be limited to terrorist offences as defined in Council Framework Decision 2002/475/JHA and to crimes falling within the competence of Europol.

---

[8] Proposal for a Decision of the European Parliament and the Council establishing the European Refugee Fund for the period 2008-2013 as part of the General programme "Solidarity and Management of Migration Flows"

As far as the comparison of DNA profiles is concerned, the limitation to a hit/no hit check against the sole DNA profile (alphanumeric chain of number without any other personal information) allows the principle of proportionality to be respected fully.

The principle of proportionality is of particular relevance when it comes to the creation of a European register for travel documents and identity cards. It must be noted that all relevant data protection authorities including those that welcome the creation of national registers, have recommended not implementing a European register, due to the potential for abuse. The creation of such a register should therefore only be envisaged if access is strictly limited and if searching the register is justified by an overwhelming and imperative public security interest.

Last but not least, as regards all possible measures, it must be emphasised that comprehensive supervision by competent data protection bodies will be indispensable. In any case, when putting forward possible future proposals, the Commission will proceed, in accordance with Communication COM (2005)172[9], to a specific impact assessment on the respect of fundamental rights.

[9] Comunication of 27 April 2005 COM (2005)172 final on the Compatibility of legislative proposals with the chargter of Fundamental Rights (setting out a methodology for the internal control of fundamental rights, their integration in impact assessment depending on the scope of the likely impacts and inclusion of a standard recital on the Charter)