COUNCIL OF THE EUROPEAN UNION

Brussels, 2 October 2012

14157/12

LIMITE

JAI 638
DAPIX 114
CRIMORG 109
ENFOPOL 289
ENFOCUSTOM 92

NOTE

from:	Europol
to:	Working Group on Information Exchange and Data Protection (DAPIX)
No. prev. doc	17748/11 JAI 888 DAPIX 164 CRIMORG 229 ENFOPOL 289 ENFOPOL 156
Subject:	Target information management architecture (IMS Action 10) - Draft vision on EU law enforcement information exchange

Delegations will find attached to this note the draft vision on EU law enforcement information exchange submitted by Europol as the outcome of the work done in the Working Group on IMS Action Point 10. It has previously been presented at the DAPIX meeting of 11 January 2012 and at the COPE Conference of 25-27 April 2012. Changes with regard to the previous document (doc. 17748/11 JAI 888 DAPIX 164 CRIMORG 229 ENFOPOL 289 ENFOPOL 156) are set out in bold in order to facilitate the reading of the document.

It is stressed that the implementation of this vision over time will require concrete initiatives, specific timelines and a common engagement to implement them. In this respect account should be taken of concrete proposals contained in the Commission Communication on the EIXM to be tabled end of 2012 where the Communication follows the lines of this vision. Furthermore, DAPIX can take up an important governing role in the identification and prioritisation of future Action Points to ensure compliance with the framework set by this vision.

Delegations are invited to discuss this document at the DAPIX and to provide comments in writing.

Draft vision on
EU law enforcement information exchange

1. Introduction

This vision is (…) **the main deliverable** of **the Project Group on** the *Target EU Information Management Architecture*, which is listed as Action Point 10 for the implementation of the EU Information Management Strategy. The IM Strategy was adopted by the Council in December 2009[1].

The aim of this vision is to set the direction for developments of information management related initiatives within the EU that support cross-border law enforcement cooperation. As such, it should provide DAPIX with a (…) perspective against which it can assess the relevance, need and compliance of new legal instruments and proposals for future information management tools. **In this respect it also provides direction for** (…) **designing concrete (…) recommendations to improve law enforcement information exchange** (…) **within the EU (…) to be taken into consideration in the framework of defining the EIXM by the end of 2012.**

(…) **In order to reconcile effectiveness and respect for fundamental rights and in particular the right to data protection, it is essential that initiatives which are implemented following this vision are accompanied by** (…) **in-depth impact privacy assessments. This** (…) concerns in particular **the concept of cross-matching (para. 3) and the information exchange platform (para. 6)** (…). **In any case the output of impact assessments should allow to chose the implementation alternative that provides for the effectiveness required while ensuring the highest level of data protection.**

2. General principles

Information exchange between law enforcement authorities within the EU is based on a spirit of cooperation and mutual support to achieve the best result possible **for the fight against** (…) crime and terrorism that affect Member States.

Information exchange in the context of EU law enforcement cooperation will at all times respect the fundamental rights of citizens, in particular where it concerns the protection of personal data. Due care and attention is given to ensure that law enforcement staff as well as their policies, processes and processing tools will fully comply with the applicable legal, security and data protection requirements.

---

[1] see Council Conclusions on an Information Management Strategy (doc. 16637/09 JAI 873 CATS 131 ASIM 137 JUSTCIV 249 JURINFO 145)

The design of the regulatory framework, the working processes and information management tools are aimed at maximising the efficiency and effectiveness of information exchange supporting EU law enforcement cooperation. Simplicity and common standards are key facilitators to achieve this objective.

3. Availability of information

In accordance with the Principle of Availability, information must be managed in such a way that it is without undue delay available for law enforcement authorities throughout the EU for the prevention and combating of crimes and terrorism that affect the security in Member States. **Access to personal data is protected by the fact that the right to access data is granted on a "need to know" basis depending on the data or categories of data being accessed, the duties of the people allowed access, the purpose of the access or processing operation to be carried out.**

To achieve this objective, it is essential that relevant links between data sets across the EU are identified and actively managed. This means that **relevant** crime related databases managed at EU level **and** by Member States are, **where appropriate,** indexed[2] (…) in a (…) manner **that allows for identifying** (…) related information (…) as input for coordinated law enforcement action. (…) As such, available data can be linked automatically or on decision, **on the basis of respective legislation and r**especting the purpose of data collection, data retention limits, proportionality and restrictive measures imposed to protect sensitive investigations and intelligence operations.

The need to identify links between data also applies to the various information exchange initiatives. So, if there are for instance links between data exchanged in the framework of Prüm and data exchanged through Police-Customs Cooperation Centers (PCCCs), then these must be found and taken into consideration for the handling of the case.

The full picture of the crimes concerned is important for the proper handling, including the choice of the cooperation channel, and is likely to facilitate solving the matter more efficiently. It is also of particular importance for the proper implementation of intelligence led policing.

---

[2] The **outcome of the feasibility study on a** European Police Records Index System (EPRIS), **which will be finalised by second half of 2012,** could contribute to this service; (…) **as far as required functionalities like** search and cross-matching mechanisms are already in place, **existing systems should be considered before developing new ones** (Principle of Convergence).

Therefore, all related information must be combined as soon as possible so that it allows choosing the appropriate law enforcement response already in an early stage of investigation. Depending on the subject matter the most effective form of cross-border cooperation may be bilateral, for instance through the SIRENE Bureau or a PCCC[3], or multilateral through a regional initiative such as MAOC-N[4] **or CECLAD-M**[5] or a cooperation mechanism organised at EU level, like Europol. In addition, it must be possible to shift easily to a more appropriate level of law enforcement cooperation should the case in question turn out to be of a different proportion than anticipated.

For the acceptance of such a large scale interlinking of data, it is probably necessary for most law enforcement information to design the exchange mechanism as a hit/no hit process. This implies that a decision at national level of the requested state is needed to (…) disclose the information that triggered the hit.

Although this could have a considerable impact on resources, still the workload will be kept under control by applying information exchange standards (Universal Messaging Format – UMF2 Project) that can enable the automation of several standard manual processes. The information exchange standards can also facilitate the cross-matching itself to identify the links while ensuring compliance by means of embedded security and data protection settings, like data retention periods and access restrictions.

Not all information will require a hit/no hit process. Those types that need less protection can be made available directly to law enforcement officers, even at regional or local level. It is obvious that this makes the workload much more manageable and avoids central bottlenecks. However, decisions on the level of protection imposed will have to be made by the authority that makes the data available.

The conditions to be met in order to implement the envisaged information exchange perspective described above, are elaborated in the following paragraphs.

---

3 **A PCCC can also be organised as a multilateral cooperation framework between more than 2 Member States.**

4 Maritime Analysis Operational Centre - Narcotics.

5 Centre de Coordination pour la Lutte Anti-drogue en Méditerranée.

4. Coordination

Effective coordination mechanisms are necessary at various levels to reach the intended level of cross-border information exchange within the EU and with relevant partners, such as non-EU States and Interpol.

4.1. Coordination **of international cooperation** within Member States

The coordination within Member States concerning cross-border information exchange is considered as the cornerstone for EU law enforcement cooperation. The combination of sufficient competent staff, effective tools and efficient processes should allow for the adequate management of cross-border information flows. This applies not only to the coordination of specific areas, such as Europol, Interpol, SIS/SIRENE, FRONTEX, regional cooperation and Prüm, but also to the coordination between these cooperation frameworks. In particular, the coordination between cooperation channels is important. Duplication of effort, miscommunication and overlooking important links must be avoided. A consistent use of instruments and channels, combined with training of staff and automated notification of links should be considered as minimum safeguards.

The follow-up to identified matches between data of the Member State with that of different Member States and other partners requires swift action from the coordination functions within a Member State. That way the investigators on the ground can benefit from receiving the related information from abroad as well as from any other support that eases their cooperation with foreign law enforcement authorities.

The coordinaton and swift follow-up to identified links would benefit from the establishment of Single Points of Contact (SPOCs) in all Member States and from the accessibility for these SPOCs to all relevant data repositories within their Member State. To enable the SPOC to take up a pivotal role in the exchange of information, clear coordination arrangements are required with all relevant national instances.

4.2. Interagency coordination

EU Agencies[6] have been established in several domains of law enforcement to provide a multilateral answer to crimes that affect Member States at a transnational level. The division of tasks between EU agencies involved in law enforcement requires their close cooperation and coordination to ensure that the Member States can rely on a well-concerted support. Especially at EU level, it is important to complement the national perspective of crime phenomena and developments with an overarching picture. This means a lot more than just a sum of national statistics. It implies that there is an in-depth knowledge and actual understanding of crimes, criminals and criminal developments that affect the security in the Member States from an international dimension. It also implies the need to be granted access to the information on which this knowledge and understanding can be based.

Due to their broad mandate Europol and Eurojust can play a central role in the cooperation between the EU Agencies and coordinate the joint response to the Member States' needs for assistance. Europol can drive the cooperation in terms of criminal intelligence and investigations, whereas the emphasis of Eurojust involvement lies on judicial coordination and cooperation. In their coordinating role, Europol and Eurojust must cooperate closely with other EU Agencies in those domains where their areas of competence meet.

4.3. Coordination outside the EU

Law enforcement cooperation outside the EU can be divided in two categories: non-EU Schengen countries and other partners. The non-EU Schengen partners are in many respects treated as EU States and will be considered accordingly **in the context of this vision**.
For the other cooperation partners, a combination of bilateral cooperation and a multilateral approach organised at EU level should be applied, based on the nature of the case that is being addressed. Crimes from outside the EU that affect multiple Member States require a multilateral response, including information exchange, analysis and operational support. In cases where a multilateral approach is required to combat threats from outside the EU, a close cooperation between, in particular, Europol and Interpol is essential for an effective joint approach.

---

[6] This includes FRONTEX, OLAF, CEPOL, Eurojust and Europol. Although OLAF is technically not an Agency, it is also considered as part of this group.

Concerning the exchange of personal data with external partners, due consideration shall be given to the adequacy of the applicable data protection framework and the respect for human rights.

5. Interoperability

Significant improvement of information exchange can only be achieved if the conditions for processing data are simplified, streamlined and standardised. Enhanced interoperability is needed in various respects, such as the legal framework, information management tools, policies and working processes.

5.1. Complementary set of streamlined legal instruments

Effective information exchange requires a coherent set of legal instruments to support EU law enforcement cooperation. (…) **T**hese instruments should cover the entire spectrum of business needs to combat cross-border crime that affects security in the EU. For business needs that are not yet addressed, either existing instruments must be adapted or specific new ones must be created to fill these gaps.

The set of legal instruments must also avoid offering any redundancies. In case the user can choose between instruments to achieve the same purpose, the consistent use of the available tools is at risk. This will affect the smoothness of cross-border cooperation as well as the ability to effectively monitor and steer law enforcement.

Furthermore, to the extent possible the set of legal instruments must be consistent in terms of security and data protection requirements, access rights, and the allocation of responsibilities. In general, this makes it easier in terms of compliance, training and implementation. In addition, it offers more possibilities for combining different legal instruments or switching from one to another, if needed.

For instance, there are only minimal differences in the crimes listed in the European Arrest Warrant (EAW) and those listed in the Annex to the Europol Council Decision. The legal framework of Eurojust refers to the crimes for which Europol is competent. The Swedish Framework Decision refers both to the EAW and to the competences of Europol and Eurojust. This calls for simplification and streamlining.

Similarly, the cooperation between law enforcement and judicial authorities should also be based on a coherent, aligned and streamlined framework of legal instruments. The **cooperation and workflow between law enforcement and judicial authorities should be organised in a practical manner in terms of common deadlines, actions, communication and decisions, both at national level and in case of cross-border cooperation (…)**. **This interoperability of legal instruments** must allow for a seamless connection **between** law enforcement and judicial processes (…)

5.2. Interoperability at business level

To guarantee efficient cross-border cooperation, aligned business processes and workflows are to be implemented at national and EU level. These business processes and workflows must be designed as simple and homogeneously as possible, while containing the necessary security and data protection safeguards.

In this respect, already much work was done in the composition of various handbooks and guidelines that structure several domains of cross-border law enforcement cooperation.

Also guidelines for selection criteria, specification of required competences, training and screening of staff working in the domain of international law enforcement cooperation will enhance the quality, compliance and effectiveness of international information exchange.

5.3. Semantic interoperability

In addition to the previous points, information exchange should be further enhanced by alignment of data processing. Standardisation and simplification should be achieved in the area of the evaluation of reliability of sources and information as well as the conditions/restrictions for the handling of information.

Furthermore, in support of common work processes, interoperability between information management tools should be based on an agreed information model and related information exchange standards (UMF2 Project). Security and data protection safeguards must be embedded in the metadata of exchanged information. Combined with standardised roles and access profiles these will enhance assurance and compliance auditing.

5.4. Interoperable technical architecture and processing tools

EU law enforcement and judicial authorities should have an interconnection of secure, reliable, interoperable and scalable networks. This infrastructure should be made available to all relevant actors in an efficient manner without unnecessary redundancies. Efficiency gains can be achieved by a consolidation of existing solutions.

From an interconnected secure infrastructure between the EU Agencies a single onward connection to national networks **should be established to provide for the option to communicate with several Agencies and Member States at the same time, instead of having a different network interface to each EU Agency. The combined, secure infrastructure should interconnect (to the extent required) all relevant partners at national and international level, including SPOCs, PCCCs, EU Agencies, Interpol, regional initiatives and liaison officers posted abroad.** (…)

This common infrastructure should give access to a complete set of national and international processing systems. Such tools are expected to facilitate the exchange of information, data storage and cross-matching with a strong focus on enabling coordination at national level and the enforcement of access controls, security and data protection. In other words, users should have the necessary processing tools at their disposal, that complement each other in such a way that they accommodate all business needs for cross-border information exchange in a fully compliant manner.

For these information management tools also applies that there should be a minimum of overlaps and a maximum coverage of the law enforcement domain. The latter refers in particular to the capability to reach any law enforcement information of relevance for cross-border cooperation and making it available for that purpose in a meaningful way.

Last but not least, agreed standards are necessary for the collection and use of statistics on the exchange of information. Statistics should not only cover qualitative data, such as the instruments that were used, but also provide quantitative figures on the exchange of information. Comparable statistics are not only a must for proper management of information exchange tools, but can also serve as a relevant source for strategic crime analysis.

6. Centralised access to relevant data and processing tools

Law enforcement practitioners will benefit of a clear and complete overview of available legal instruments, information management tools, sources and cooperation channels.
The consistent use of these instruments will be ensured by agreed criteria for their application, adequate training of staff and, where beneficial, by automation.
Controlled access to the repository of instruments for cross-border law enforcement cooperation **should be** granted through a common information exchange platform **as currently designed in the IXP project**. This portal **would need to** guide practitioners to required information and assist in the selection of the most suited tools and cooperation channels on the basis of the individual needs. In this process, national policies, procedures, authorisation and routing **should** be observed, while access rights, security and data protection compliance **should** be enforced.

This portal **should** also assist investigators to find relevant information across the EU. In this respect, the portal **should** re-direct duly authorised officers to the general search and cross-matching capabilities envisaged, as also referred to in paragraph 3. **The follow-up mechanisms for retrieving relevant data identified via the IXP will need to be integrated with the national coordination through SPOCs, as presented in paragraph 4.1, to ensure the required swiftness, compliance and quality control.**
