COUNCIL OF
THE EUROPEAN UNION

Brussels, 16 December 2010

11117/3/10
REV 3

LIMITE

JAI 546
DAPIX 36
CRIMORG 120
ENFOPOL 167
ENFOCUSTOM 54

NOTE

from:	Europol
to:	Working Party on Information Exchange and Data Protection (DAPIX)
No. prev. doc.	7752/10 ENFOPOL 70 CRIMORG 61 ENFOCUSTOM 23
Subject:	Business Concept for an Information Exchange Platform for Law Enforcement Agencies - (IMS Action 4)

1. Introduction

In January 2010 the Spanish Presidency of the Council of the European Union presented a proposal to establish at EU level an information exchange platform for law enforcement agencies to the Ad Hoc Working Group on Information Exchange. This topic was taken up in the Action List of the EU Information Management Strategy (Action point 4).

As a first step it was decided to specify the concept of the information exchange platform and to identify concrete steps for developing the platform (cf. doc. 7752/10 ENFOPOL 70 CRIMORG 61 ENFOCUSTOM 23). This task was commended to a small group, led by Europol and Spain.
The current document presents the business concept for the information exchange platform, including the impact on the work of law enforcement officers and the added value it offers.

The more technical aspects will follow once the business concept is clear. When the technical details and practical consequences, including the specific data protection and security safeguards, have been further elaborated, the relevant stakeholders, including data protection authorities, will be consulted prior to any realisation**. The questions addressed in the next stage are listed at the end of this document.**

The re-use of existing solutions (or those under development) and other efficiency considerations reflected in the IM Strategy will be applied in order to reduce the costs of development, running and maintenance.

2. Purpose

The information exchange platform (IXP) is designed to improve law enforcement cooperation at EU level by facilitating smooth access to relevant tools, channels, information and law enforcement partners **in accordance with (inter)national provisions and conditions for such access.**

3. Scope

The IXP will serve as a single, secure gateway to available information, products and services of relevance to cross-border law enforcement cooperation involving EU Member States and potentially associated third countries. The establishment of any new system processing personal data is not intended.

End-users are dispatched from the IXP to existing products and services where relevant. The applicable rules, governing access rights, authorisation, security and data protection compliance will be fully respected and applied mutatis mutandis with the establishment of the IXP. This implies that end-users will be granted access to the IXP only in accordance with national or other applicable procedures. The same applies to their access to systems, channels and other services to which they are re-directed from the IXP.

4. Key Features

The IXP is distinguished by a number of essential characteristics that are listed and elaborated below:

- Single platform: the main element of the concept is a single website that serves as the starting point for any product or service related to international law enforcement cooperation. This approach has several advantages, such as efficiency in development and maintenance, easier management of data protection, the enhancement of a shared experience as well as the user-friendliness of recognising and easily finding contacts and services in other Member States.

- Available for staff of ~~any~~ law enforcement bodies in the EU: in accordance with the EU Information Management Strategy (IMS) the IXP is targeted to the end-user and intended for the entire law enforcement community in the EU. This includes local, regional and national police forces, customs, coast guard and border control authorities. Also international law enforcement bodies, like FRONTEX, OLAF, Interpol, EMCDDA, CEPOL, EuroJust and Europol should have access. It can also be extended to other institutions, such as DG JLS, the Council Secretariat General, but also judicial, prosecution and penitentiary services, where relevant. In principle, even non-EU partners could be given access, like the non-EU Schengen partners Norway, Iceland, Liechtenstein and Switzerland**. The extent to which users get access to the various parts of the IXP is subject to the decision of the applicable (inter)national authorities responsible for these users.**

- Access to relevant products and services: the single platform should provide any available answer to operational needs for cross-border law enforcement cooperation. To this end the IXP gives access (or re-directs) to relevant tools, channels, and information without affecting the applicable access management, security or data protection measures in place. It also assists the end-user in finding the appropriate products and services on the basis of the concrete needs for cross-border law enforcement cooperation. The possibilities can be divided in 4 categories: Knowledge Management, Tools, Operational Queries and Communication Channels.

  Knowledge Management:

  ► General information: users may be directed to documentation needed in general as background information or to understand how certain matters are organised. One can think of legislation, forms, policy documents, tutorials, handbooks and guidelines, for instance for the so-called Prüm Decisions or the Swedish Framework Decision.

  ► National information pages: for each Member State, but potentially also for associated third states, one or more information pages could be made available. These web pages can provide details on the law enforcement structure, data protection authorities, legislation, national peculiarities as well as contact points for specific types of support and cooperation.

► Information pages of EU bodies, agencies and networks: similar to the national information pages also the EU law enforcement bodies such as OLAF, FRONTEX, EuroJust and Europol, **(…)** the European Union Crime Prevention Network as well as data protection authorities like the European Data Protection Supervisor and the joint Supervisory Body, should have their information pages available on the common platform. The Council Secretariat General and DG JLS can publish relevant information. Also CEPOL could provide the platform with contents related to training.

► Expert communities: for more specific purposes dedicated environments can be made available to enable law enforcement experts to communicate among each others on their area of competence. These domains can be used to share experience, modi operandi, statistics, risk assessments, training material, best practices, specialised law enforcement techniques, specific solutions and contact lists. The communication can be supported by discussion fora and collaboration tools. These opportunities are linked with the establishment of the Europol Platform for Experts.

Tools:

► EU law enforcement tools: the IXP will be useful for joint investigations teams, joint police and customs cooperation, common police teams and patrols, major event teams (e.g. for football championships), EU law enforcement missions abroad, etc.

► Shared tools: the IXP can give access to tools that were jointly developed or made available for common use. Such tools could for instance be used for data mining, analysis or the monitoring of the internet and open sources consultation. For some of them dedicated joint initiatives are currently being set up closely related to the establishment of the IXP.

► Translation: for cross-border cooperation translation is a key factor, but also a complicating one. The specific terminology would justify the establishment and maintenance of a police dictionary and a glossary (thesaurus). Also a list of abbreviations used in law enforcement would be beneficial. **Within the limits of feasibility specific** ~~Sufficient~~ care should be taken to **prevent impediments** ~~avoid any~~ impediment caused by language barriers.

► News service: it could be considered to create a news service that publishes live news of relevance to cross-border law enforcement cooperation.

Operational queries:

► The platform should enable a search capability that processes queries across the relevant databases managed in the framework of justice, liberty and security, and potentially also national databases. The processing must respect access restrictions established in the respective legal framework of the different data bases, as well as any other **national provisions and** applicable data protection conditions. Applicable measures to prevent unauthorised use or access will be assessed for effectiveness and complemented where necessary. **Due attention will be paid to aligning this feature with existing and developing initiatives.**

Communication channels:

► Under the applicable conditions for access rights and national coordination the IXP can also re-direct to the communication channels used for cross-border information exchange, such as Interpol I24/7, SIRENE and the Europol communication tool SIENA.

In particular with regard to the operational queries and the communication channels the detailed elaboration of the technical and practical aspects to be made in the next stage will clarify how this relates to existing and developing initiatives and their respective legal, security and data protection frameworks.

5. Added Value

The establishment of the IXP will make it easier for end-users to benefit from the existing opportunities for cross-border law enforcement cooperation, while respecting the national and international processes in place. The platform gives access to required information, products and services that officers on the ground are looking for when it comes to international law enforcement cooperation.

Moreover, it even assists the user to identify the appropriate (legal) instrument(s) and communication channel(s) on the basis of the concrete needs this officer has. **By defining a question or the specifics of a case the IXP can refer the user in accordance with the national conditions and procedures to the applicable legal framework, the appropriate contact details and required products and services.** Apart from offering a complete package of tools and information, the IXP also has a strong focus on the user experience to ensure that any consultation of the platform quickly leads to the aimed result.

As a consequence, it is expected that the platform will enhance the use of international products and services to support investigations**, while respecting the (inter)national arrangements for coordination and compliance**. In addition, the informative character and the assistance to find the right instruments will contribute to the quality of communication in general and products and processes in particular. And as such, the IXP will contribute to the increase of successful cross-border law enforcement cooperation and will represent a major step towards a common law enforcement culture within the European Union.

6. Conditions

To make the IXP actually work a number of conditions has to be observed. At least the following aspects have to be taken into consideration:

- National conditions: any involvement of a Member State, whether it concerns the usage by any of its staff or access to any of its products and services, is subject to national discretion, respecting domestic legislation, policies and arrangements.
- Security: the security levels vary depending on the classification of environments, products and services. The security requirements for accessing the various parts of the platform or being forwarded to any other environment will have to be met before access is granted. Access to current services is not changed and additional access is granted in accordance with the existing policies. For additional services dedicated policies will be implemented by the authority responsible for the service in question.
- Data protection: for as far as the processing of personal data is concerned the applicable data protection safeguards will be applied and monitored by the applicable data protection authorities. In addition, any existing data protection issues with the applicable systems will be mapped and assessed in advance. For additional services (e.g. the news service) the necessary data protection measures will be designed and implemented in consultation with the respective data protection authorities. Auditing and access control features of the platform will be accessible to the relevant data protection authorities, who could benefit from the uniform and centralized architecture of the IXP. These logs shall only be made available for the purpose of auditing.
- Language: it is essential that an effective solution is found to bridge language differences, while respecting resource constraints of law enforcement authorities. Using a common language would seem most efficient. National languages can be supported to the extent that Member States support translation, without prejudice to those contents directly provided by Member States in their own national language. Some services are less dependent on translation. For the search function, for instance, the look-up values and search fields can be displayed in various languages. However, for services where information is published at least an abstract with key words should be made available in a common language.
- Management: the IXP will be developed, supported and maintained in close consultation with its stakeholders and representatives of its user community. Responsibilities will be assigned concerning the project management for the gradual realisation of the IXP and with regard to the product management for the operation, content management and maintenance of the solution throughout its lifecycle.

7. Next Stage

First agreement is sought on the business concept for the IXP as presented in the previous paragraphs. This addresses *what* the IXP is expected to offer. Once this agreement has been reached then in the next stage an assessment is made of *how* this can be achieved. At that stage the possibilities for the design of the solution are considered. The next stage will should enable to answer the following questions:

- **How are the key business processes organised? This includes user authorisation; access levels; identity and access management; user roles; maintenance of the various environments; compliance with national provisions on coordination; routing and re-direction to existing products and services; auditing; division of responsibilities.**
- **How can these business processes be supported by ICT solutions? The options for the technical implementation will be assessed with a strong focus on re-use of existing and developing IM tools as well as on security and data protection safeguards.**
- **What are the costs for the development and maintenance of the IXP? In the comparison of technical solutions also the financial aspects will be taken into account.**
- **What will be the timelines of the development of the IXP? It is most likely that a gradual approach will be taken for the implementation of the IXP. On the basis of the chosen technical solution a roadmap can be defined with the concrete steps towards the progressive implementation of the IXP.**

An answer to these questions will serve as input for informed decision making on the way forward, including the aspect of *who* will be involved in terms of governance, delivery, maintenance and funding.