COUNCIL OF
THE EUROPEAN UNION

Brussels, 25 November 2009

16637/09

JAI 873
CATS 131
ASIM 137
JUSTCIV 249
JURINFO 145

"I/A" ITEM NOTE

from:	General Secretariat
to:	Coreper/Council
No. prev. doc.	15857/09 JAI 825 CATS 121 ASIM 127 JUSTCIV 237 JURINFO 142
Subject:	Draft Council Conclusions on an Information Management Strategy for EU internal security

1. On 26 June 2009, the Presidency submitted a proposal to the Ad Hoc Working Group on Information Exchange for an Information Management Strategy. The aim of this strategy is not to define what kind of information should be stored and/or exchanged but the strategy rather provides a methodology (the “how”) to ensure that decisions about the need for managing and exchanging data and decisions about the ways to do so are taken in a coherent, professional, efficient, cost-effective way, accountable and comprehensible to the citizens and the professional users. It is not a legally binding text.
When put together with the EU's priorities in Justice and Home Affairs and in particular in internal security[1] (the “what”), the Information Management Strategy will allow the relevant authorities to implement in an efficient and effective manner the future developments in information exchange policy.

[1] A Member State may decide to apply this strategy by adopting a step-by-step approach, for instance by limiting its application to specific sectors of internal security such as law enforcement and judicial cooperation in criminal matters. Where that Member State has experienced that the approach of the strategy should also be applied to other sectors, it can decide to expand its application.

2. The strategy is the top document and as such has a long-term focus. It can be further developed and updated as the overarching vision develops or changes and should be reviewed by the end of 2014. The Information Management Strategy will be complemented by an action list/road map defining concrete goals, processes, roles and deadlines.

3. The Ad Hoc Working Group on Information Exchange examined the proposal in detail in its meetings of 7 and 13 July, 26-27 September, 15 and 26 October and reached general agreement on the text, subject to some reservations on the scope of the document. The Article 36 Committee discussed the proposal in its meeting of 10-11 November 2009 and agreed on the draft Council conclusions, subject to outstanding reservations of CZ, DE, AT and LT.

4. Coreper discussed the draft Council conclusions in its meeting on 20 November 2009 and invited the concerned delegations to lift their reservation. This was done subsequent to the meeting.

5. **Coreper is therefore requested to invite the Council to approve the draft Council conclusions on an Information Management Strategy for EU internal security, as set out in Annex.**

6. At the request of the DE delegation, the following declaration will be added to the minutes of the Council approving the Council conclusions:

   Germany fully supports and endorses the idea laid down in The Hague Programme (doc. 16054/04, sub III. 2.1) and in The Hague Action Plan (doc. 9778/2/05 REV 2, sub 3.1. lit. k)) to adopt and implement an EU Information Management Strategy. Germany therefore supports and endorses the Council Conclusions on an Information Management Strategy adopted today as far as cross border information sharing among law enforcement and judicial authorities dealing with criminal matters within the existing legal framework of the EU is concerned.

THE COUNCIL OF THE EUROPEAN UNION,

RECALLING

– the Hague Programme on strengthening freedom, security and justice in the European Union[2], in particular section 2.1 that calls for improved exchange of information to fight crime and therefore establishes the principle of availability,

– the Council and Commission Action Plan implementing the Hague Programme on strengthening freedom, security and justice in the European Union[3], in particular point 3.1.(k) that calls for a definition of a policy for a coherent approach on the development of information technology (IT) to support the collection, storage, processing, analysis and exchange of information,

– the report of the Future Group of ministers for home affairs, recommending the implementation of a "European Union Information Management Strategy" (EU IMS) to remedy to the current situation of an "uncoordinated and incoherent palette of information systems and instruments" which have "incurred costs and delays detrimental to operational work" and thus going "beyond the limited perspective of a case-by-case approach and aim for a holistic objective in law enforcement information management.",

– the Council conclusions on the principle of convergence and the structuring of internal security[4] and the follow-up on the outcome of the Informal JHA Ministerial meeting in the field of Modern Technologies and Security[5],

[2] Document 16504/04 JAI 559

[3] Document 9778/2/05 REV 2 JAI 207

[4] Document 14069/08 JAI 514 CATS 78

[5] Document 10143/09 JAI 324 CATS 55 ASIM 54 ENFOPOL 145 CRIMORG 85

- the European Commission's Communication of 10 June 2009, entitled "An area of freedom, security and justice serving the citizen" (COM(2009)262), which states that security in the EU depends on effective mechanisms for exchanging information between national authorities and other European players,

- the European Council's acknowledgement in the Stockholm Programme of the need for coherence and consolidation in developing information management and exchange, inviting the Council to adopt and implement an EU Information Management Strategy, entailing business driven development, a strong data protection regime, interoperability of IT systems and a rationalisation of tools as well as overall coordination, convergence and coherence**,**

BUILDING UPON

- the work accomplished by the Friends of the Presidency[6] on the technical modalities to implement the principle of availability,

- the proposed Council Conclusions[7] on the definition of a policy for a coherent approach on the development of information technology (IT),

- conclusions of the 2007, 2008 and 2009 COPE conferences[8] and the Common Requirements Vision[9],

[6] Document 13558/1/05 REV 1

[7] Document 15478/05 CRIMORG 152 CATS 87

[8] Documents 10063/07 CATS 70, 13592/08 CATS 74 and 14033/09 CATS 99

[9] Document 7758/08 CATS 21

RECOGNISING THAT

Effective and secure cross border exchange of information[10] is a precondition to achieve the goals of internal security in the European Union.

This requires the right information to be available at the right time, for the right person and in the right place. Tasks of internal security are divided across a range of authorities (the "business" side) and this division is different from one Member State to the next, depending on national structures, competences and legal framework. All too often in the past, decisions on information exchange have been made dependent on organisation – to – organisation grounds, not allowing for these structural differences between Member States and resulting in unnecessarily complicated requirements for information exchange.

The Hague Programme established the principle of availability as the vision for the exchange of information in the EU and specified that, to do so, "the methods of exchange of information should make full use of new technology and must be adapted to each type of information".
Consequently, in order to promote exchange between Member States and facilitate the practical modalities thereof, the relevant information should be available in an appropriate format, requiring that national decisions take account of EU policies. Moreover, the Member States and authorities involved need a high level of trust in one another's management of information.
The principle of availability also requires citizens' expectations of privacy to be balanced against their expectations of security.

Considering the panoply of existing instruments for cross-border information exchange, Member States have at several occasions expressed the need for coherence and consolidation and a need to implement existing instruments and arrangements rather than embark upon new initiatives. This demonstrates the need to professionalise and streamline the management of information, including the collection, storage, processing, analysis and exchange.

[10] In this context, information means information and criminal intelligence required by the competent national authorities and available to them under the relevant regulatory framework for the objective of improving the EU internal security of the EU citizens.

This need for coherence and professionalization is exacerbated by the growing mobility of citizens, the increasing complexity of crime phenomena and hence the EU policies to counter them, as well as by the necessity for the EU and the Member States to maximise their resources.

The Information Management Strategy aims to support, streamline and facilitate the management of information necessary to the competent authorities to ensure the EU internal security but excluding the responsibilities of Member States in safeguarding their national security. The authorities concerned will be essentially law enforcement authorities, authorities responsible for border management and judicial authorities dealing with criminal matters. However, the need for information exchange with other authorities and sources will also be taken into account.

There is a clear need to distinguish between the methodological tools used to manage information efficiently and the goals and reasons for processing thereof**.** The latter (the "business vision and needs") follow from the political priorities set by the Council, notably in the Stockholm programme.

HEREBY RESOLVES

1. To adopt and implement an Information Management Strategy with a view to supporting, streamlining and facilitating the management of information necessary to the competent authorities to ensure the EU internal security, which

   a) is based on the following principles:

   – information management is an essential tool in realising the objectives of increasing the EU internal security and protecting its citizens, but it is not a purpose in itself and remains a means to an end. Priorities set for information management and exchange must correspond to political, policy and operational priorities and support the business vision on how to realise the above-mentioned objectives;

- information management is functionally defined, i.e. depends on the task to be carried out, as opposed to competence-based or organisationally defined. It follows that the EU Information Management Strategy provides for the multidisciplinary approach needed to develop an Area of Freedom, Security and Justice**,** notably the potential of enhanced information exchange and closer cooperation between all the parties involved in order to increase efficiency in the fight against cross-border crime;

- the strategy provides guidance on how to ensure an appropriate information exchange where supply of information takes account of both business needs and the rights of the individual. It defines the preconditions for the professional, business driven, efficient and cost effective development and management of information exchange. The strategy shows the way towards a structured information exchange and forms a basis for enhanced decision making processes and governance;

- the strategy in itself does not create links between different databases or provide for specific types of data exchange, but it ensures that, when the operational requirements and legal basis exist, the most simple, easily traceable and cost-effective solution is found;

b) consists of eight focus areas grouped under the following headlines and elaborated in annex:

I. Needs and requirements
  1. Needs, requirements and added value are assessed as a precondition for development
  2. Development follows agreed law enforcement workflows and criminal intelligence models
  3. Development supports both data protection requirements and business operational needs

II. Interoperability and cost efficiency
  4. Interoperability and co-ordination are ensured both within business processes and technical solutions
  5. Re-utilisation is the rule: do not re-invent the wheel

III. Decision-making and development processes
  6. Member States are involved from the very start of the process
  7. There is a clear responsibility for each part of the process, ensuring competence, quality and efficiency

IV. Multidisciplinary approach
8. Multidisciplinary coordination is ensured within the JHA area

2. To take the necessary steps to develop and update as necessary a detailed action plan in order to fulfil the overall aims and objectives of this strategy.

INVITES

– preparatory bodies of the Council dealing with issues of information exchange and IT development to implement the strategy

– COREPER to task the Ad hoc Working Group on Information Exchange to draw up an Action List for implementing the Strategy as well as to ensure, on the basis of reporting by that and other working groups, the coherent and efficient implementation of the strategy

– EU officials and Member States representatives and experts in EU structures and agencies to take account of the strategy in their work preparing decisions, including on information exchange on a bilateral or regional level and with third countries or organisations; and to consider the strategy when preparing and running programmes and projects for information exchange and IT development

– Member States to support the common efforts at EU level by adopting the strategy at national level as guidance for policy makers, Chief Information Officers and other decision makers in their competent authorities when dealing with issues related to or influenced by cross-border information exchange and IT development (including "national housekeeping" and dealings with third countries or organisations)

– the Commission to apply the methodology agreed upon in these conclusions when drafting a Communication that supports the Council in formulating a business vision to enhance information exchange for law enforcement purposes and elaborating its European Information Exchange Model.

I. NEEDS AND REQUIREMENTS

1. Needs, requirements and added value are assessed as a precondition for development.

This focus area sets out the requirement for an assessment of added value before any new information exchange is established. It also reflects the vision of the availability of information based on purpose, necessity and proportionality.
It will require an assessment of the business needs as well as business and legal requirements for the concerned co-operation, including how the solutions will be used, and how useful they will be for enhancing the actual operational co-operation and working methods.
As a consequence, development will be based on and driven by the needs and requirements of the authorities involved. An assessment of usefulness (including cost/benefit analysis) will also help to set priorities for development.

This means that:

a) *when initiatives regarding information exchange or technical solutions are put on the agenda, end-users and the management level in different areas need to be involved. Without their support it is impossible to assess the importance and value of an initiative. Their participation is also relevant when it comes to clarifying the balance between data protection and business needs;*

b) *ideas or discussions regarding technical solutions have to be subordinated to the analysis of needs and requirements;*

c) *work on legislative instruments and/or pre-studies for technical solutions should not start before the business requirements are identified and documented;*

d) *any initiative in the field of information exchange has to be based on an in-depth analysis of existing solutions on the EU level and in the Member States, the definition of needs, requirements and the added value as well as assessment of the legal, technical and financial impact of the new initiative;*

e) *clear assessment criteria, supported by systematic evaluation programmes should be developed;*

f) *assessment of the usefulness in developing for example specific information types should derive from a strategic prioritisation process.*

2. Development follows agreed workflows and criminal intelligence models.

Improving the exchange of information relies heavily on support from IT solutions. For IT to support information exchange, it has to support the business processes of cross-border law enforcement co-operation.
Business processes must allow the quick, efficient, user friendly and cost-effective exchange of information and criminal intelligence. The work flows must therefore be described, known and accessible. They should be an integral part of the work to develop and procure systems. As a consequence, there will be better management and documentation of development and the needs of cross-border law enforcement co-operation will steer development.

This means that:

a) *work on the existing Common Requirements Vision (CRV) should be continued and complemented by analyses of substantial requirements, made together with and by national authorities;*

b) *an "information map" should provide an overview of business processes and the corresponding information flows of cross-border co-operation, so as to identify on that basis the interfaces at which coordination is needed.*

3. Development supports both data protection requirements and business operational needs.

Cooperation with a view to ensuring the EU internal security places high demands on data protection including data security. Personal privacy as well as business security have to be ensured, while providing for business needs to use and share information.

A high level of security will protect business interests as well as citizens' private lives, without reducing the availability of information, so that correct information is available to authorised users in a traceable way, when needed and permitted by existing legislation. Adequate use of modern technologies, but also adaptation of business processes and measures to implement data protection, facilitate this. Enhanced trust in these areas between competent authorities is an important step towards an attitude of data-sharing by default.

This means that:

a) *the legal requirements for protection of personal data and for security standards must be assessed together with business needs for use and exchange of information, so that the right levels of business and technical security standards are ensured for information exchange and IT systems;*

b) *data collection must be well targeted, in order to protect personal privacy as well as to avoid information overflow for the competent authorities and facilitate efficient control over the information;*

c) *data security must be ensured through organisational as well as technical and physical means;*

d) *the different tools, such as applications and support tools, must be rationalized with a view to simplifying the work of the competent authorities and the end users; this will minimize the risks of damage, as will training about the available tools and their use;*

e) *adequate measures to implement data protection must provide for proper and regular operational checks and ensure that appropriate sanctions are effectively applied in the event of any breach;*

f) *systematic evaluation and monitoring mechanisms should be developed to assess the quality and the effect of data protection and data security measures.*

II. INTEROPERABILITY AND COST EFFICIENCY

4. Interoperability and co-ordination are ensured both within business processes and technical solutions.

Interoperability concerns multiple levels, such as legal, semantic, business and technical levels. Interoperability is both a prerequisite for and a facilitator of efficient information exchange. Interoperable solutions and capacities build on initiatives and proposals that start from business needs and requirements.

Technically, IT solutions and their components should comply with commonly agreed standards and principles. Standard solutions should be used and kept to a minimum.
Their use will provide greater coherence both in the development and management of solutions. This also supports interoperability and co-ordination between systems. As a consequence, there will be better and increased use of existing solutions and IT systems will be able to support larger parts of work processes. The need for double storage and double registration will decrease and the IT support will become more user-friendly. By applying commonly agreed standards, information exchange can be supported by several suppliers rather than a few, minimizing dependence on special suppliers. In the long run it will also decrease the cost of adaptation in Member States.

This means that:

a) *the "information map" should include a comparative overview of EU and Member States legal situation in the area of information exchange;*

b) *the recommendations of the European interoperability strategy should be considered;*

c) *existing, commonly agreed, accreditation/standardisation functions should be used;*

d) *integration enablers, such as standard technologies and capabilities, which facilitate integration and are designed to provide security, scalability and performance, should be identified;*

e) *measures to implement data protection and data security should be coordinated at and between both the EU and national levels.*

5. Re-utilisation is the rule: do not re-invent the wheel

Development means high costs and considerable investment, but also long-term costs for management, maintenance and support. Normally, only a small part of the total cost is used for the development phase. This is not an issue only for technical development, but also a question about not creating new legal bases or practical arrangements, when existing ones can be used or extended.

As a consequence, sharing and re-utilisation of sustainable solutions must be a priority for development and technical improvement. Re-utilisation helps to avoid parallel solutions and to further develop existing instruments and systems, their integration and usefulness. As a consequence, there will be increased use of past investment and less need for new investment. The time necessary for development will also decrease the more components are at hand.

Efficient re-utilisation requires an "information map", providing an overview of existing information flows, functions and components. Efficient (re-)use of successful solutions also requires a constant evaluation process and a follow-up mechanism for assessing how the exchange of information operates.

This means that:

a) *the "information map" should include information flows, functions and solutions;*

b) *an evaluation mechanism that is pragmatic, relevant and resource-effective must be presented. It should be purpose- and not competence-based; it should not be limited to certain (legal) instruments and it should be ensured that lessons learned from evaluation can be implemented;*

c) *to assess the impact of its work, the EU must create tools to measure not only criminal activity but also the effects of its efforts, notably the development of information exchange, on the EU internal security;*

d) *a model of how to share and re-use sustainable solutions should be produced taking account of practices from within the EU but also from third countries;*

e) *a critical review of instruments currently in use for information exchange should assess their efficiency and effectiveness in order to allow for a rationalisation and certainly before starting to develop new tools.*

III. DECISION MAKING AND DEVELOPMENT PROCESSES

6. Member States are involved from the very start of the process.

Decisions at EU level about cooperation, information exchange and IT development have a substantial impact, in a short as well as a lifecycle perspective, on Member States' business processes, structures, investments and budgets. A fully functional end result requires intensive coordination at national level as well as reciprocity and interaction between the national and EU levels.

Member States' authorities, which are responsible for national implementation of workflows, methods and development have to be involved from the beginning of the development processes at European level. To be able to contribute fully, Member States should work on their own interoperability, both business and technical, and establish their own development processes.

This means that:

a) *national and EU information management strategies or policies should be in line with each other;*

b) *end-users and key stakeholders should be involved at both the national and EU level;*

c) *authorities in Member States need to identify and develop their own development processes.*

7. There is a clear responsibility for each part of the process, ensuring competence, quality and efficiency.

In order to better steer the development process, the roles and responsibilities of the actors involved must be clarified. Special competences are needed in different areas, such as business and technical architecture, methods and models, management, finance and control. Discussions about (technical) solutions must be kept on a level with the right technical and architectural competence. Decisions on management and political levels have to address the appropriate issues for that level.

This means that roles must be identified, responsibilities defined and structures set in place to ensure that all parties concerned are involved at the right level and at the right stage of the process, but also that there is overall coordination and coherence.

This means that:

a) *roles and competences on different levels (within national authorities, EU institutions, bodies and agencies etc.) must be identified and organised;*

b) *functions to prepare the strategic decisions on information management and IT development have to be identified/established;*

c) *functions for management, further development and evaluation of (business and technical) solutions must be in place.*

IV. MULTIDISCIPLINARY APPROACH [11]

8. Multidisciplinary coordination is ensured.

The Information Management Strategy recognises and caters for the multi-disciplinary approach necessary to achieve internal security and to facilitate the transfer and re-utilisation of information, independently of the body holding the information. Modern technology makes it possible to achieve the desired level of availability, which in turn can minimize disruption and manual re-registration and increase the quality of information. The same technology makes it possible to maintain or increase the level of data protection, including data security.

The strategy aims to facilitate the functionalities and technicalities of information exchange between relevant authorities if and when this is legally provided for. Thus, the strategy calls for and provides means to ensure interoperability.

This means that the efforts to achieve interoperability require interaction between all the relevant authorities and organisations. Which authorities and organisations will depend on the specific need that is catered for. The methodology set out in this strategy and in particular focus areas 1 to 3 will ensure that interoperability is ensured whenever necessary and proportional, among and beyond the authorities directly responsible for the EU internal security, but also that it is limited to these cases.

[11] **Study reservation: DE**

This means that:

a) *information exchange must not be hampered by issues of competence (mutual recognition of different national structures) while fully respecting the applicable legal framework for such information exchange;*

b) *IT support and standardisation (including architecture principles and information/data models) must be as horizontal as possible and based on common principles and coordination;*

c) *measures to implement data protection and data security should be coordinated between the EU level and Member States.*