Sweden 17 October 2007

INFORMAL HIGH-LEVEL ADVISORY GROUP ON THE FUTURE OF EU HOME AFFAIRS POLICY (THE FUTURE GROUP)

Discussion paper on the essentials of a European information network in 2014

I. The subject

1. Terrorism and organised crime will remain a threat to the European Union and its citizens in the coming years. The Union will therefore have to be particularly vigilant in demonstrating its capacity to drive forward policies at EU-level and by working together with law enforcement and judicial services in the daily efforts to meet this challenge. Consequently, the work of the Future Group can and should be a significant contribution for the elaboration of the planning of an EU home affairs policy towards 2014.

2. In preparing the meetings of the Future Group during spring 2007, a series of challenges for the future were identified[1]. With the aim to enhance the exchange of information, the questions on what the essentials of a European information network in 2014 are and how to take advantage of information technology compose one of the challenges identified.

3. This paper is a contribution to the discussions on this challenge from the perspective of crime fighting and crime prevention co-operation in the EU. The aim is in particular to put some questions for discussion with a view to highlight some possible avenues or actions for achieving a co-ordinated and coherent implementation of the principle of availability (the PoA) towards 2014. It seems that such a development is in line with the general view expressed by ministers at Eltville in May.

4. Put in more detail, the paper seeks to identify a series of actions on how to address a very complex challenge with a view to progressively clarify its contours and to attaining the following objectives:

- the application of a coordinated and coherent approach to the implementation of the PoA aiming at a professional, business-oriented and cost-effective use of information technology and information networks;
- the establishment of law enforcement business processes which can facilitate the quick, efficient and cost-effective means for exchanging and making information available; such processes to be accountable and incorporate a robust data protection;
- the establishment of technical solutions for law enforcement business processes that are designed to meet current and future business needs, including to maximize its functionality and interoperability as well as its openness to expansion and modification.

[1] Document of the Co-chairs, 30 March 2007

5. However, it should be recalled that home affairs are at the core of each Member State. This is for instance an issue of current interest as regards the proposed Framework Decision on data protection in the third pillar and “ownership” of law enforcement intelligence and information. It is also true that national security is a responsibility incumbent upon Member States and to which extent matters of national security forms part of this exercise is open to discussion.

II. The Principle of Availability and work on its implementation by October 2007

6. The PoA means that, throughout the Union, a law enforcement officer in one Member State who needs information in order to perform his duties should be able to obtain this from another Member State and that the law enforcement agency in the Member State which holds this information will make it available for the stated purpose, taking into account the requirements of ongoing investigations in that State. The PoA can therefore, as is the case with the principle on mutual recognition for judicial co-operation, be said to be a cornerstone and a vision for law enforcement co-operation. Since the essentials of a European information network taking advantage of information technology is embedded in the PoA, some key elements of its implementation so far should first be reviewed.

7. By October 2007, the work of the JHA-Council and its working structures on the implementation of the PoA involves a number of legal initiatives, reports, Council Conclusions etc. A first step to implement the PoA, representing the classic “police-to-police approach”, i.e. indirect access to information upon request, was taken on 18 December 2006 by the adoption of the Framework Decision on simplifying the exchange of information between the law enforcement authorities of the EU[2]. In connection with the discussions on the Framework Decision a total of 49 types of relevant information (annex 1) were identified and each Member States legal possibilities to make them available. An overview was presented in February 2005[3].

8. Further steps to implement the PoA are mainly concerned with the use of information technology. At present, the incorporation of the Prüm Treaty into the EU acquis is the most concrete example regarding the PoA and technical means to exchange information (DNA, fingerprints and vehicle registration). Other examples include the work under way within Europol on an Information Management Strategy (IMS), including the PoA, and an Information Communication Technology (ICT) Strategy, SISone4all and SIS II, law enforcement services access to VIS and EURODAC, work within the EUPCTF on a Common Requirements Vision (IT-development to be driven by law enforcement business needs) etc.

9. Out of these relevant processes, the work within Europol on an IMS and the work under forerunnership of Bundeskriminalamt on a CRV for the EUPCTF provide future oriented prospects as they both are examples of modern, state-of-the-art approaches on how to address the complex matter of information management. The purpose of an IMS is to support the needs of law enforcement strategies by describing communication and information flows, including by means of information technology. An IMS must also ensure interoperability and alignment of the strategies and IT investments. In this way the IMS serves as a guideline for single technology decisions.

[2] OJ L386/89, 29.12.2006

[3] CRIMORG 7, 5815/2/05

The purpose of the CRV in turn is to identifying the needs or requirements of the law enforcement services in terms of access to information and intelligence. A CRV comprises a look at for instance societal developments, crime trends, modii operandi and law enforcement strategies such as intelligence led policing. On this basis, the aim is to define the law enforcement business needs as precisely as possible and in turn the demands on information technology to support the work processes.

10. A more detailed assessment of the technical modalities available (annex 2) for implementing the PoA was taken note of by the Council on 1 December 2005, i.e. the report of Friends of the Presidency[4] (FoP-report). Besides developing the objectives enshrined in the PoA (reflected in point 4 above), the FoP-report focuses on six types of information, i.e. DNA; fingerprints; ballistics; vehicle registrations; communications data; and minimum data for the identification of persons contained in civil registers. The approach contained in the FoP-report is a reflection of the agreement by the Council on 14 April 2005 to apply a progressive (data field-by-data field) approach to the implementation of the PoA starting with the mentioned six types of information.

11. Furthermore, in conjunction with the presentation of the FoP-report, a proposal for Council Conclusions[5] was presented on the 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. Such conclusions are called for by point 3.1.(k) of the Council and Commission Action Plan on implementing the Hague Programme. The background of the proposal is to be found in the need to ensure for instance that the processes leading to technical solutions will ensure that present and future demands on interoperability and integration are considered. The proposal has by October 2007 not been discussed in Council working structures.

12. On 12 October 2005, the Commission also submitted a proposal for a Framework Decision on the exchange of information under the PoA. The proposal covers DNA; fingerprints; ballistics; vehicle registrations; telephone numbers and communications data (with exceptions); and minimum data for the identification of persons contained in civil registers, i.e. the same types of information selected for the progressive approach and in part covered by the Prüm Treaty. It is proposed in the Framework Decision as a main regime that direct online access is provided by each Member State to other Member States' law enforcement authorities as well as Europol officers. By October 2007, the proposal has not been discussed in Council working structures.

13. This said, it is also worth recalling that already before the establishment of the PoA, the Article 36 Committee concluded in November 2002 that the overview of the IT-development to support law enforcement exchange of information was becoming blurred. As a consequence, an ad hoc study on the third pillar information systems was presented in May 2003[6]. The study provides an inventory of existing and planned law enforcement IT-systems at EU-level at that time.
The Article 36 Committee concluded that there was a broad opinion in favour of continuing the work and expressed a general preference for the option: "To investigate and implement the

[4] CRIMORG 112, 13558/05

[5] CRIMORG 152, 15478/05

[6] JAI 118, 8857/03

harmonization of the data formats and their respective access rules between the various systems while allowing current systems to evolve to provide interoperability between them". By October 2007 further work on the basis of the ad hoc study has not been initiated.

14. Finally, data protection principles should be strictly observed when implementing the PoA and the proposal for a Framework Decision on the protection of personal data, presented already in October 2005, is intended to meet the requirements of the Hague Programme. It can be expected that discussions on the Framework Decision can be concluded in the near future.

III. Taking stock of the implementation of the PoA by October 2007

15. It is obvious that the implementation of PoA is a complex subject matter that requires thorough reflection and discussion. Besides obvious political considerations, the implementation of the PoA raises a number of other important issues, i.e. issues of a legal, organizational and technical nature. In addition, a solid data protection regime is a prerequisite for the implementation of the PoA, both in terms of general provisions on key conditions and for specific types of information and the technical modalities applied.

16. Relevant documents and work highlighted above illustrates that the first steps have been taken and that the level of activity is quite high, but that there is further work to be done on additional types of information (cf. the 49 types identified above under point 7), technical modalities etc. should the vision of the PoA be fulfilled.

17. The work so far undertaken also reveals that the implementation to some extent is scattered and dealt with by different working structures representing different starting points. This can be exemplified by the work to develop the exchange of information extracted from criminal records. Although this type of information is highly relevant both for law enforcement investigations and the criminal justice system, the work undertaken within criminal justice working structures is not coordinated with work carried out in home affairs structures. Other examples demonstrate not only the reversed situation, but also that within home affairs structures the level of co-ordination is not sufficiently catered for. Furthermore, the only dedicated working group for exchange of information so far, i.e. the Ad Hoc Group on Information Exchange, only met a few times before its work was overtaken by the incorporation of the Prüm Treaty. Such a forum would provide a platform for matching the professional, business driven IT-development evolving within Member States law enforcement services.

18. Turning to the development of IT to facilitate the exchange of information, the need for enhanced co-ordination and coherence is also clear. To date, experiences show that the development of IT-tools to support the exchange of information at EU-level have been quite a challenge and work currently under way have encountered many difficulties causing unnecessary costs and delays. There is therefore a need to ensure that upcoming solutions devised consider present and future demands, and do not constrain future expansion and modification, i.e. a business driven and proactive approach.

19. Furthermore, a continuation of the work undertaken by the ad hoc group for the study of the third pillar information systems would provide information on what databases and other knowledge banks exist, the types of data stored, the retention periods, the various access regimes

etc. Indeed, establishing and maintaining an overview of the third pillar information systems seems imperative for a coherent approach to the implementation of the PoA.

20. Finally, the new financial framework for 2007-2012 should be paid attention to. The allocated budget under the Security heading will increase by 968% over the period and for 2008 the indicative financial distribution for the incorporation of the Prüm Treaty and the PoA will be 9.290.000€. This development is significant and provides new opportunities.

IV. Questions for discussion aiming at highlighting some possible avenues or actions towards a co-ordinated and coherent implementation of the principle of availability

21. Political and legal framework

- Should we reflect on how to design a political and legal framework in order to define the preconditions for the exchange of information in the European Union within the "triangle" between mobility rights – security needs – data protection? Should the Commission's proposal for Framework Decision on the PoA aiming at direct online access be part of such reflections?

22. The venue

- Should there be a dedicated working group on Information Exchange established with a view to providing a forum with the mandate to taking forward the continuous implementation of the principle of availability in a co-ordinated and coherent manner?

23. The map

- Should the work be pursued on a continuous overview on the EU law enforcement and judicial information systems providing an inventory of existing and planned IT-systems in order to ensure that the capabilities of these systems are fully exploited and overlapping mechanisms and duplication are avoided?

24. The compass

- Can a set of basic principles or guidelines form the basis for a law enforcement business driven IT-development, i.e. a coherent approach within the third pillar (cf. the proposed Council Conclusions on the definition of a policy on the development of (IT))?

25. Information Management Strategy

- Should an EU Law Enforcement Information Management Strategy (IMS) be developed with a view to translate law enforcement business needs into a systematic planning for IT-development (ICT) to support such business needs?

26. Progressive approach (information types and technical modalities)

- Should the work on the agreed progressive approach (data field-by-data field) be pursued by an assessment of the added value, appropriate technical modality etc. for the identified 49 types of law enforcement relevant information on the basis of the methodology developed by the Friends of the Presidency[7] (FoP-report, annexes 1 and 2)?

- Out of the 49 types of information: Which do we need most and which priorities can be identified, e.g. a top 10 list?

- In which cases do central databases for law enforcement data generate an added value?[8] In this respect should we apply an added value test particularly referring to efficiency, feasibility, financial or economical considerations? Which criteria could be decisive for whether we should:
    - create central databases,
    - access the data on a hit/no hit basis,
    - access the data directly from one MS to another,
    - access the data indirectly upon request?

- Generally, to what extent should "non police data" be accessible for police purposes (current examples being Eurodac or EU-PNR)? Should this generally be possible in cases of grave offenses or imminent danger?

27. EU-financing

- Should the use of information technology for the enhancement of exchange of information as well as for a better protection of personal data be considered a priority issue for annual financial allocations?

- Should we acquire or use state-of-the-art technical equipment jointly on an intergovernmental or EU basis without thereby limiting Member States' sovereignty (e.g. equipment needed for monitoring open sources of information on the internet such as the check the web project)?

28. External dimension project or reference

- Should we develop a more integrated approach/strategy with third countries as the external component of a European information network with the aim to further enhance exchange of information between the EU and third countries?

[7] CRIMORG 112, 13558/05

[8] N.B. The Hague Programme foresees that that new centralised databases should only be created on the basis of studies that have shown their added value.