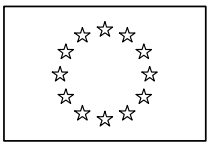

COMMISSION OF THE EUROPEAN COMMUNITIES

Brussels,
COM (2004) 429/4

Draft

**COMMUNICATION FROM THE COMMISSION TO THE COUNCIL AND THE EUROPEAN PARLIAMENT**

**Towards enhancing access to information by law enforcement agencies**

(presented by the Commission)

# TABLE OF CONTENTS

# COMMUNICATION FROM THE COMMISSION TO THE COUNCIL AND THE EUROPEAN PARLIAMENT TOWARDS ENHANCING ACCESS TO INFORMATION BY LAW ENFORCEMENT AGENCIES (*EU INFORMATION POLICY*)

## CHAPTER I– INTRODUCTION, RATIONALE AND POLICY CONTEXT

### Overview

The declaration of the European Council on terrorism[1] instructs the Council to examine legislative measures to simplify the exchange of information and intelligence between the law enforcement authorities of the Member States. The Commission is invited to bring forward proposals to the June European Council in relation to exchange of personal information and the use of passenger information for the purpose of combating terrorism. The Commission proposals should also include provisions to enable national law enforcement agencies to have access to the European information systems.

The present Communication is a first contribution from the Commission in response to the request from the Council.

In this Communication, the Commission sets out the elements that are critical to achieving free circulation of information between the law enforcement authorities of the Member States, in a more structured way than has been the case up till now, Obstacles to free circulation of information currently exist, which cause *inter alia* the Council to dedicate the third round of mutual evaluations to examine the "exchange of information and intelligence between Europol and the Member States and among the Member States respectively". Compartmentalisation of information and lack of a clear policy on information channels hinder information exchange. The challenges to overcome the division of information between different Ministries nationally are exacerbated by the legal, technical and practical problems hindering exchange between Member States. In order to obtain a more accurate picture of these obstacles, the Commission proposes to undertake a full stock-taking exercise on the conditions to access information, as well as a broad and open consultation with all interested stakeholders namely the European Data Protection Supervisor. The Communication also aims to provide the means of avoiding the materialisation of major threats, such as terrorism, by introducing the concept of intelligence-led law enforcement at EU level. It provides an agenda setting out how to achieve this, and it announces legislation to remove specific legal problems. The focus of this Communication is improvement of access to necessary and relevant information, as well as on the broad concepts for the introduction of intelligence-led law enforcement at the level of the EU. This will also have consequences for the international role that the EU is able to assume.

These two elements are the building blocks of the EU Information Policy for Law Enforcement. Common action in these fields will support the progressive establishment of the area of freedom, security and justice, in which the free movement of persons remains assured in the face of the new security challenges that terrorism and other forms of serious and organised crime pose to the Union as a whole. Effectiveness of law enforcement activities should build upon observance of human rights and fundamental freedoms as protected by international,

[1] European Council of 25 March 2004 *Declaration on combating terrorism*.

European and constitutional traditions common to Member States. Furthermore, while building this policy, the Commission will ensure that Community law and policies are duly taken into account. In particular such a policy should not create legal uncertainty or undue economic burdens on industries.

The Commission calls on the Member States and involved parties to engage in the following bold, cooperative actions.

Firstly, to take the indispensable steps to make accessible necessary and relevant data and information for EU law enforcement authorities, in order to prevent and combat terrorism and other forms of serious or organised crime as well as the threats caused by them.. In this respect; it should be borne in mind that often criminal activity that would not appear to come within the category of "serious or organised" can well lead or be connected to it.

Secondly, to produce and use high quality EU criminal intelligence. Knowledge that will become available in this process will assist the political level in setting EU law enforcement priorities in a concerted manner, and the law enforcement authorities to confront effectively the crimes and threats that jeopardise our citizens' lives, physical integrity and security.

Thirdly, to enhance trust between enforcement services. The introduction of common conditions for instance to access data systems, and the sharing of know-how will contribute to set up a joint information policy platform in particular by removing objective obstacles to the effective sharing of information and intelligence.

A number of considerations drive the EU Information Policy for law enforcement. They are related to the growing awareness of the vulnerability of the Union to threats like those posed by terrorist activities to the dependence of the Union on interlinked networks; to the need to establish enhanced information flows between competent authorities, to the benefits of new technology and knowledge-based capabilities in boosting law enforcement action and, at the same time, enhance data protection, security, and related monitoring and supervisory mechanisms.

This communication intends to improve information exchange between all law enforcement authorities, *i.e.* not only between police authorities, but also between customs authorities, financial intelligence units, the interaction with the judiciary and public prosecution services, and all other public bodies that participate in the process that ranges from the early detection of security threats and criminal offences to the conviction and punishment of perpetrators. The fundamental role that State security and national intelligence agencies play in this regard is undisputed. The many *inter-linked* challenges that the EU Information Policy for law enforcement intends to address are presented in the following paragraphs.

Finally, the external dimension must be taken into account, because of the international nature of the challenge of terrorism and organised crime that we are trying to address. Other countries have developed or may develop in the future their own Information Policies for Law Enforcement and we have already seen cases where those policies have implications for EU citizens and economic operators. Reciprocity issues may also arise. And multilateral solutions may have to be sought in specialised forums. The impact that the EU Policy would have on the nationals of third countries will also need to be properly taken into account, to ensure both that law enforcement cooperation with those countries is not impaired and that the rights of citizens are respected without discrimination.

***This policy will firstly make accessible the necessary and relevant data and information, for law enforcement authorities in order to prevent and combat terrorism and other forms of serious or organised crime as well as the threats caused by them[1]. Secondly, it will foster the***

[1] For the purpose of this Communication the expression "data" or "information" means "data, information and intelligence" unless otherwise indicated; the term 'intelligence' refers to 'criminal intelligence'.

***production and use at EU level of high quality criminal intelligence to assist the political decision-making and the law enforcement authorities in effectively confronting these crimes. Thirdly, it will support the building of trust between the competent services. While building this policy, Community policies and Community law instruments will also be taken into account; in particular this policy will fully respect fundamental rights.***

**The Information Policy has to take account of the following elements:**

- The **security** challenge requires as a matter of necessity common and concerted action on an unprecedented scale,; the stakeholders are the national law enforcement authorities, national governments, the European executive and legislature, and other bodies at European and international level.

- The **human rights** challenge means striking the appropriate balance between robust data protection and due respect of other fundamental rights on the one hand and, high performing use of law enforcement information aimed at safeguarding essential public interests such as national security and the prevention, detection, and prosecution of crime on the other.

- As concerns **technology**, compatible information systems protected against unlawful access with appropriate data protection, including the monitoring and supervision of data processing and the auditing of investigation are needed. Crime-proofing of information technologies should expose weaknesses and opportunities for criminal activities and focus on data analysis such as risk assessment and profiling.

- To facilitate effective **co-operation**, common standards for information collection, storage, analysis and exchange will critically support the building of confidence between the competent services, both at national and EU level.

- The **implementation** of a multi-phased approach will require the need for long-term sustained cooperative action.

## CHAPTER II – TOWARDS BETTER ACCESS TO DATA AND THE INTRODUCTION OF INTELLIGENCE-LED LAW ENFORCEMENT AT THE LEVEL OF THE EU

### 2.1. Strategic objectives

The objective of this Communication is to establish an EU Information Policy for law enforcement that will contribute to the realisation of the objectives of Art 29 TEU by providing better information over secure channels for **existing law enforcement cooperation** and laying the groundwork for the **establishment of effective intelligence-led law enforcement** at local, national and European levels, underpinned by the necessary **trust building**. The policy plan is encompassing legal, technical and organisational actions that, taken together, will provide law enforcement authorities with a framework for cooperation in order to facilitate the access to and the processing of data relevant for law enforcement and to produce criminal intelligence.
When looking in more detail at the Information Policy the intended results are to:

- optimise access to information to further core law enforcement activities as well as to produce criminal intelligence;

- ensure that relevant data established for other than law enforcement purposes be available as long as appropriate, necessary and proportionate to the specific and legitimate purposes pursued[1];
- set up or, in case of already existing horizontal standards, promote the effective use of common horizontal standards on access to data, clearance, confidentiality of information, reliability, data security and data protection, and interoperability standards for national and international databases;
- establish agreed intelligence formats to assist political and operational decision-making and promote the development and use of equivalent methods for the analysis of e.g. criminal networks, crime threats, risks and profiles, to be further supported by economic harm assessments;
- provide the basis for the prioritisation of the EU-wide collection and analysis of information and, subsequently, for the selection of the best course of action in order to prevent and combat terrorism and other forms of serious or organised crime as well as the threats caused by them, within the set priorities;
- facilitate cooperative and coordinated law enforcement action with a view to prevent, investigate, or disrupt, effectively and as appropriate, terrorist activities and activities dealing with other forms of serious or organised crime.

***Improved access to data, information and intelligence will support law enforcement in each Member State and at European level in order to prevent and combat terrorism and other forms of serious or organised crime, as well as threats caused by them. Additional added value will occur when data is methodically analysed in order to produce first-class criminal intelligence. To support EU intelligence-led law enforcement, minimum standards for national criminal intelligence systems should be adopted, enabling compatible threat assessments at European level.***

## 2.2. Core elements for effective access to and collection, storage, analysis and exchange of data and information

### *2.2.1. The principle of equivalent access to data between law enforcement authorities*

The first core objective of the Information Policy for Law Enforcement is to establish free movement of information between law enforcement services, including EUROPOL and EUROJUST. At present, law enforcement authorities can search databases that are nationally accessible. However, accessing information held by law enforcement services from other Member States poses challenges that amount to making them inaccessible in practice.

The Information Policy aims at making this information practically accessible to all EU law enforcement authorities, including EUROPOL and EUROJUST, to assist them in the execution of their functions and in accordance with the rule of law.

The principle that the Information Policy introduces to offset the challenges put forward in the previous chapter is the one of **'right of equivalent access to data'.** This would give EU law enforcement authorities and officials equivalent rights of access to data and databases within other EU Member States on comparable conditions as law enforcement authorities in that Member State. The corollary to that right is the obligation to provide access to law enforcement

[1] A legislative proposal on data retention has been tabled by four Member States at the April 2004 JHA Council. The Commission foresees an open consultation on the matter.

officials of other Member States under the same conditions as national law enforcement officials.

***This implies a commitment from Member States to act within a EU model comprising issues such as the synchronisation of threat assessment based on a common methodology and systematic underpinning of threat assessment by sectoral vulnerability studies.***

The principle of equivalent access recognises that:

– the security of the Union and its citizens is a joint responsibility,

– Member States depend on each other to enforce laws in order to prevent and combat terrorism and other forms of serious or organised crime, and contain the threats caused by them ;

– law enforcement authorities in one Member State fulfil similar tasks and have equivalent information needs as those in other Member States;

– law enforcement authorities act lawfully when accessing data or querying databases in the execution of their tasks and within the boundaries set by common standards on data protection and data security.

As a matter of principle, the right of equivalent access should not diminish the effectiveness of existing Mutual Legal assistance instruments. Any potential legal effects will have to be carefully analysed.

***Transparent and straightforward conditions for accessing the necessary and relevant information for all EU law enforcement authorities should be set up based on common standards, including on data protection and data security. Member States will be responsible for the implementation of these conditions. A system to monitor the implementation will be set up following the identification of the conditions for access in the course of the stock taking exercise (see paragraph 2.2.2).***

***Core obstacles to the exchange of information between law enforcement authorities can only be effectively addressed on the basis of a firm commitment of Member States to take concrete measures towards the setting up of a European Criminal Intelligence Model (see paragraph 2.3).***

***The European Information Policy aims at the introduction of the principle of right of equivalent access to the necessary and relevant data and information for EU law enforcement authorities. The Commission will examine with Member States which obstacles exist and, on this basis, assess the appropriateness of submitting a legislative proposal to the Council and the European Parliament related to its introduction at EU level.***

*2.2.2. Scoping of the conditions for access*

The Commission proposes to carry out a full stock-tacking exercise on the basis of available information as well as on information provided to that end by Member States, to chart the following elements:

– which data or databases are accessible to law enforcement authorities in Member States and which ones are accessed abroad, including index databases (*content*);

– what is the purpose of the database *(purpose definition)*;

– which kind of law enforcement authority has access to these data (*users*);

– under what conditions do these authorities have access to these data and databases (*access protocol*);

– what are the technical requirements for access to these data and databases (*technical protocols*);

– how often are the data and databases accessed (*relevance*);

– which data or databases are of interest to law enforcement authorities, but are not accessible to them; what are the applicable data protection provisions (*scoping of needs*).

**The Commission intends to:**

– ***launch a stocktaking exercise by the end of 2004, to identify the scope, needs and constraints of access to data and databases by law enforcement authorities.***

– ***launch a study on legal provisions, conditions, including IT solutions to access (non-) law enforcement data, , and procedures related to data protection and data security provisions.***

### *2.2.3. Data collection*

The law enforcement authorities in the EU use diverging approaches to collect and categorise data and information. No single forum for the classification of the confidentiality of different information sources exists at this moment.

The first and foremost information source is the data collection of the law enforcement administrations. Access to data not collected for law enforcement purposes is another policy issue. It requires a broad and open consultation with all interested stakeholders, in view of its possible implications on operators and users and on Community laws and policies.

A system to manage the different access privileges such as common *European standards for the authorisation to access classified information*, a joint system of *users access profiles* to administer the numerous access rights, and an authenticated way to register authorised users (cf. *users accounts*) would provide the basis for an effective access management. User profiles could also be used to systematically monitor and audit the access to and processing of data that could be kept in *log files and audit trail* systems.

***The Commission intends to launch studies to underpin the elaboration of legislative and non-legislative initiatives related to minimum standards for the collection of data; common procedural standards to classify the confidentiality and the reliability of data; common standards on the authorisation to access classified information, and user access profiles.***

***The Commission will further organise consultations and multi-disciplinary workshops under the EU Forum on the Prevention of Organised Crime to discuss public private partnerships and in particular on the access to data not collected for law enforcement purposes.***

### *2.2.4. Data exchange and processing*

Besides different ways to access data and databases on the basis of the principle of equivalent access, another option to make existing data and data bases better accessible is by networking them or creating central databases. In this context the European Council[1] invited the Commission "to submit proposals for enhanced interoperability between European databases (SISII, VIS and EURODAC) in order to exploit their added value within their respective legal and technical frameworks in the prevention and fight against terrorism"[2]. Enhanced

[1] European Council of 25 March 2004 *Declaration on combating terrorism*.

[2] A separate Commission Communication will be prepared on this subject.

interoperability will need to take due account of the applicable legal provisions on data protection.
The Commission is of the view that the only viable option for the future will be the creation of interoperable and interconnected EU systems. A conceptually comprehensive IT architecture that integrates national, European and international inter-linkages offer in the long run considerable savings, synergies and policy opportunities, both in the area of criminal intelligence and in the broader context of an evolving European Security Strategy.
A phased approach should be conceived based on the setting up of harmonised data encoding formats and access rules for the various systems. Early consultations with stakeholders conducted by the European Commission[1] have already identified a number of issues that may pose obstacles to information sharing. These include in particular the lack of:

- common standards and conditions for data processing;
- common data accessibility standards;
- compatible crime definitions and crime statistics;
- compatible IT technologies used by law enforcement administrations;
- co-operative law enforcement cultures beyond institutional borders;
- co-operation between public and private sector actors;
- awareness of common data protection rules and a lack of a common data security framework.

***The Commission envisages submitting a communication to explore effective ways to remove core obstacles that cause impediments to data sharing and which will, as appropriate, be supported by respective legislative initiatives.***

*2.2.5. Research*

The current European research programmes address the issue of security of information and communication systems and infrastructures. The Commission has already considered the need to accelerate the preparation of a European Security Research Programme to improve European citizens' security by launching a Preparatory Action on Security Research[2]. The 'Preparatory Action for Security Research', which is defined for the years 2004-2006 (budget € 65M) would support and finance activities to test the ground in view of the comprehensive European Security Research Programme from 2007 onwards.
Terrorism and organised crime are identified as the two top concerns of European citizens (80 % of EU-citizens identify terrorism and organised crime as their major fears). At present, research activities related to criminal intelligence systems or law enforcement are not sufficiently covered by research programmes. Hence, there is a need to define specific research actions in addition to existing programmes. In addition co-financing of research activities is also possible under the AGIS programme.

- ***Promote research on secure and confidential communication channels through the AGIS programme;***
- ***Initiate the development of standards for the secure exchange of information, especially by and between law enforcement authorities;***
- ***Launch specific research on the use and the implementation of European criminal intelligence systems, including on related common standards for meta-data, secure data exchanges, enhanced data protection tools, automated analysis, threat -, risk assessment and profiling methods.***

[1] Dublin Declaration and Conclusions of meetings of the Forum for the prevention of Organised Crime.
[2] COM (2004) 72 fin.

## 2.3. Core elements of an effective intelligence led law enforcement capability at EU level

The second core objective of the Information Policy is to propose steps to develop EU intelligence-led law enforcement. Criminal intelligence assists the competent authorities in the performance of their strategic or operational tasks, in order to prevent and combat terrorism and other serious or organised crime, as well as the threats caused by them[1]. The introduction of a European Criminal Intelligence Model would render intelligence-led law enforcement effective and allow for enhanced cooperative action. It would comprise issues such as the synchronisation of threat assessment based on a common methodology, systematic underpinning of threat assessment by sectoral vulnerability studies and the required financial and human resource allocation.

The EU Information Policy for law enforcement aims to **make the necessary information available to an EU criminal intelligence network** to generate first-class EU criminal intelligence, resulting in the periodic production of EU strategic and operational assessments. The availability of the Europol Information System will also play an important role in the development of such an EU intelligence capability.

The steps outlined hereafter should lead to a situation where strategic assessments are readily available to the decision makers in order to revise law enforcement priorities as often as necessary. In addition, operational assessments would become available to the Chiefs of Police Task Force (CPTF) providing the best available tactical knowledge to prevent or combat the threats or crime, including terrorism, as prioritised by the Council.

At this moment the EU law enforcement authorities are not guided by criminal intelligence that targets the security of the EU as a whole. Today an urgent need exists to protect EU citizens against new security risks and threats. Therefore it is imperative that EU strategic and operational assessments are rapidly made available. Equally the exchange of intelligence should be subject to the rule of law and respect for the fundamental rights of individuals.

Therefore the following two-phased approach is envisaged:

- In the short term, the Member States' criminal intelligence services should meet on a monthly basis, possibly under the aegis of Europol, to discuss their national strategic and operational assessments. Europol should contribute with all intelligence it can avail. The resulting intelligence should be collated to produce EU strategic assessments for instance twice a year, and EU operational assessments every month. The EU strategic assessments would allow the Council to set law enforcement priorities. The CPTF should hand down the operational assessments to the operational levels within national law enforcement communities.

This should, at first stage, draw on information that Member States' criminal intelligence and Europol can lawfully access on the basis of current legislation and make use of available analytical tools.

- In the longer term, the national criminal intelligence authorities can start producing criminal intelligence using standardised analytical tools on the basis of relevant law enforcement data available within the Union.

The importance of Europol would increase, since data and procedures will be more European. This would result in criminal intelligence of a superior quality as it would be more standardised

[1] *Criminal intelligence* is divided into strategic and operational (or tactical) intelligence. Strategic intelligence provides insight into the question of *what* the threats and crimes are that must be addressed and operational intelligence provides tactical guidance on *how* best to tackle and prioritise them.

and thus more widely understood. The relations between Europol, the Council and the CPTF need to adapt to the changing circumstances. At that moment, the EU will be in a position to assert itself on the international scene as a law enforcement partner with its own distinct character and quality.

The Commission envisages studying the necessary steps to establish a system for the timely production of reliable criminal intelligence assessment and to present a report to the Council by end of 2005.

Priorities will be set by the Council on the basis of strategic assessments that are developed by the Criminal Intelligence Group. Such operational assessment should offer the possibility of obtaining specific outcomes, for instance making arrests, seizing or forfeiting assets from criminal activities or undertaking dedicated efforts to disrupt a criminal group.

Commonly-used intelligence methods should be formatted to make them fit for use not only at the general EU level, but also to deal with specific trans-national or regional issues (e.g. the Baltic Sea Task Force on organised crime). The Commission and Europol should conduct a study of the different methods in use in Member States' criminal intelligence bodies and propose by end of 2005 a European analytical methodology for criminal intelligence. Connected to this, CEPOL could be requested to set up a training curriculum to teach criminal analysts to use these methods, and senior management to make best use of operational assessments. The analytical methods that are commonly used[1] should generate results that can be used to produce EU strategic and operational assessments.

- ***The ideas of this Communication could be endorsed by the Council as to take the appropriate measures for their implementation.***
- ***Under the aegis of Europol, the representatives of Member States' Criminal Intelligence entities should assemble national strategic and operational assessments.***
- ***The Council could call on the Member States to make intelligence available to Europol, and to mandate Europol to elaborate a comprehensive threat assessment. Customs and border control authorities could be instructed to coordinate the production of their intelligence with Europol.***
- ***Common crime statistics definitions and reporting standards should be developed***
- ***Common analysis methods for the production of intelligence at EU level should be developed possibly under the aegis of Europol.***

### 2.4. Building of trust

The third core objective of the Information Policy is to contribute to the building of trust between European law enforcement authorities, officials and partners by establishing a joint platform of shared values, standards and policy orientations.

The introduction of common standards is crucial to create a trusted environment for the collection, access and exchange of information (see in particular section 2.2). Common standards on data access and processing as well as compatible methodologies related to threat, risk and profile assessments will become an indispensable basis for the effective sharing of information and intelligence at strategic and operational levels. These measures will only be effective if there is persistent political support for the implementation of a **common law enforcement space** in the EU, based on compatible national criminal intelligence systems which will form together a conceptually integrated European criminal intelligence model.

[1] The methods are analysis in the fields of results, crime patterns, criminal markets, criminal networks, risks (which is used as a management tool in itself), target profiles (often called "profiling"), criminal business profiles, and demographic and social trends.

Accordingly, formal and informal working relations need to be developed in order to make the system function. Training of law enforcement personnel to share a common understanding of criminal intelligence will contribute to developing these aspects. CEPOL should play a major role in this context, in particular by:

– setting up regular training courses for potential future policy decision makers and top managers;
– elaborating a model curriculum for the training of middle managers in European criminal intelligence affairs at national levels;
– carrying out training measures related to all elements of the EU information policy.

Other measures would reinforce networking efforts, including those based on already existing instruments such as mutual evaluations, dedicated projects under the AGIS programme or activities conducted under the auspices of the Forum on the Prevention of Organised Crime.

Finally, the role of national data supervisory authorities should duly be taken into account as they will contribute to establish the necessary safeguards in support of the rule of law and provide for effective democratic control.

***Trust- and confidence-building measures and techniques are of fundamental importance (common standards and methodologies) The Commission envisages to present proposals by the end of 2005.***

***In parallel, the Council could invite CEPOL to initiate the development of a common curriculum for the training of intelligence officials.***

## CHAPTER III – LEGISLATIVE INITIATIVES LINKED TO THIS COMMUNICATION

The Commission will continue to develop policy, including legislative initiatives in the related areas of protection of personal data in the third pillar and the use of passenger information for law enforcement purposes, the latter in accordance with the principles set out in the Commission's Communication of December 2003[1].

The proposal for a Framework Decision on Data protection will establish common standards for the processing of personal data exchanged under Title VI of the Treaty on European Union in order to empower access to all relevant law enforcement data by police and judicial authorities in accordance with fundamental rights. This Framework Decision should provide a single general data protection framework for the purpose of co-operation to prevent, detect, investigate and prosecute crime and threats to security. It will establish a framework for the more specific provisions contained in the different legal instruments adopted at EU level, and will further reduce the practical differences in information exchange between Member States on the one hand and Member States and third countries on the other hand, and embedded in it a mechanism that ensures the protection of fundamental rights.

***

[1] COM (2003) 826 final of 16.12.03 on the Transfer of Air Passenger Name Record (PNR) Data. A Global EU Approach.