COMMISSION OF THE EUROPEAN COMMUNITIES

Brussels, 12.10.2005
SEC(2005) 1270

COMMISSION STAFF WORKING DOCUMENT

Annex to the

Proposal for a Council Framework Decision

on the exchange of information under the principle of availability

IMPACT ASSESSMENT

{COM(2005) 490 final}

TABLE OF CONTENTS

1. PURPOSE OF THE IMPACT ASSESSMENT

The implementation of the principle of availability is one of the key initiatives in the "Security" section of the Hague Programme. This programme, adopted by the European Council of 4 and 5 November 2005, seeks to further develop the area of freedom, security and justice. The implementation of the principle of availability should result in a situation where it is irrelevant whether or not information crosses borders. Given the potential for significant impact arising from action in this field, the Commission, in its Annual Policy Strategy for 2005, decided that an Impact Assessment should be carried out.[1]

The Commission decided to consult an external contractor, who provided the Commission with supporting services to assist the commissioning body (Directorate General of Justice, Freedom and Security) in the preparation of the Impact Assessment. These services consisted of analysing existing data, gathering additional information and providing advice, especially on the analysis of the obstacles to exchange and use of law enforcement relevant data.

This Impact Assessment aims at estimating the potential impact of various options for the implementation of the principle of availability. In that context, operational/law enforcement aspects, legal/organisational constraints, social/political and economic/financial effects will be taken into account. Furthermore, the consequences of inaction (i.e. not introducing legislative proposals nor other initiatives to establish information exchange on the basis of the principle of availability) will be assessed from a political (as the Commission was invited to do by European Council of 4 and 5 November 2004) and operational (as the law enforcement community is obliged to work with existing instruments) point of view. Among the legal constraints, data protection issues will be considered, including the proportionality of the access to larger and better targeted quantities of information, as well as issues relating to their storage and use.

2. STAKEHOLDERS' CONSULTATION

To prepare this Impact Assessment, the Commission organised a number of consultations in Brussels. On 9 and 10 November 2004 and 2 March 2005 consultations took place with officials from the Ministries responsible for law enforcement as well as with Europol and Eurojust. On 22 November 2004, 11 January and 21 March 2005 with national data protection authorities, and on 23 November 2004 and 8 March 2005 with representatives of the Civil Liberties Committee of the European Parliament, together with civil society and human rights interest groups (*inter alia* Amnesty International, Statewatch). In parallel, as it has been explained above, a comparative study was carried out by a private contractor on the obstacles to law enforcement information exchange and approaches to overcome them.

[1] 2005/JLS/036.

3. PROBLEMS IN THE CURRENT SITUATION AND THE UNION'S COMPETENCE TO ACT

The Schengen Agreement of 14 June 1985 on the gradual abolition of checks at the common borders between the Benelux countries, Germany and France aimed at the abolition of checks at internal borders. The Schengen Convention created a common area where checks at internal borders were abolished and checks at external borders for all Schengen States were to be carried out in accordance with a common set of rules. Another flanking measure of the lifting of internal border controls was the reinforcement of police cooperation to off set the potential negative impact of the lifting of internal border controls on the level of security of the participating States. Because of the integration of the Schengen *acquis* in the framework of the European Union, by means of the Schengen Protocol attached to the Treaty of Amsterdam, the character and nature of the flanking measures changed from instruments to buttress the free travel area against negative corollaries into building blocks of the progressively emerging area of freedom, security and justice (cf Art 29 TEU and 61 TEC). Currently 15 States apply the Schengen *acquis* in full. These are 13 Member States of the European Union plus Norway and Iceland. The United Kingdom and Ireland, Switzerland, and the new Member States that acceded the EU in May 2004, are currently not yet fully participating.

Furthermore, the fact the Council accepted that the United Kingdom and Ireland were permitted to join the Schengen police cooperation process without participating in the free travel *acquis* demonstrate that the nature of the police cooperation flaking measures changed because of the integration of Schengen in the Union.

The therefore accepted disconnection between free movement and intensified police cooperation shows that the role that police cooperation played in the concept of the free travel area established by Schengen has changed. It has become an autonomous component to ensure the "high level of safety" mentioned in Article 29 TEU. For that reason, improvement of police cooperation can find its direct justification in the progressive establishment of the area of freedom, security and justice. The three non-EU Schengen partners, i.e. Norway, Iceland and Switzerland take part in the Schengen police cooperation, but are not equally involved in the Council working groups on the issue of the implementation of the principle of availability and do not participate in the cooperation via Europol.

All legislative and non-legislative efforts deployed since the entry into force of the Schengen Convention and the establishment of law enforcement cooperation in the context of Title VI of the Treaty on European Union have focused on the improvement of information sharing between law enforcement authorities. Without exaggerating, information exchange can be characterised as the heart of police cooperation and in its improvement lays the key to better cooperation. None of the initiatives to improve information exchange were justified on the basis of a prior quantitative analysis of the information needs, but rather on a qualitative consideration, stating the needs originating in the law enforcement community itself or in the responsible Ministries. Subsequently, after their introduction, evaluation, if any, took the form of a compilation of established procedures (best practices, stock taking), peer review of the respect of agreed mechanisms (Schengen evaluation) or of satisfaction reviews (seminars organised, for instance, under the AGIS programme). The legislation adopted in the third pillar was triggered by such qualitative considerations from the law enforcement community itself or the responsible

Ministries. In the parliamentary debate, the content of the instruments, and especially the safeguarding of fundamental rights and principles, was subject of discussion, but not the motivation for their presentation. In the same way, the political initiatives taken by the Council in the field of law enforcement, not in the least those of the European Council in Tampere in October 1999 and in the Hague in November 2004, were all invariably geared towards "improvement" of different aspects of the law enforcement effort. They were justified by means of the aforementioned qualitative considerations.

3.1. Inefficiencies in the implementation of common principles and practices on law enforcement information exchange

The different evaluation processes have shown that in spite of the qualitative improvement of information exchange brought about by the Schengen Convention, Europol, and the introduction of area of freedom, security and justice by the Treaty of Amsterdam of 1997, the level of information exchange is still below what is deemed necessary for adequate law enforcement cooperation. The fact that the level is still unsatisfactory is confirmed by the focus on information exchange by several rounds of peer evaluations and the call on Member States' law enforcement authorities to broaden the data exchange with Europol. Moreover, the subsequent political initiatives taken to improve the situation (Tampere, the Hague Programme, and also the action plan on Combating Terrorism that the European Council adopted on 24 March 2004) systematically confirm the view that progress is necessary.

This being said, the marks of praise for the Schengen Information System (SIS) should not go without mentioning. The SIS provides for a trusted system with a great record of accomplishment that relays rapidly, securely and accurately agreed data between Member States. These data undeniable assist in the external border controls and law enforcement within their confines. However, the SIS is at its present stage a hit/no-hit system, not meant to support criminal investigations or crime prevention, and only contains a limited amount of data. For that reason, the Schengen Convention complemented the SIS with the mechanism laid down in Articles 39 and 46 to transmit other relevant law enforcement data in order to prevent, detect and investigate criminal offences.

Furthermore, the introduction of the Europol Information System offers the possibility to create a helpful tool to promote the exchange of information in relation to the subjects coming under the Europol mandate.

The legislative initiative of the Kingdom of Sweden with a view to adopting a Framework Decision on simplifying the exchange of information and intelligence between law enforcement authorities of the Member States of the European Union, in particular as regards serious offences including terrorist acts[2] clearly identifies in paragraph 6 of its preamble the inefficiencies to address, as well as the reasons to act. It states: "Currently, effective and expeditious exchange of information and intelligence between law enforcement authorities is seriously hampered by formal procedures, administrative structures and legal obstacles laid down in Member States' legislation; such a state of affairs is unacceptable to the citizens of the

[2] 2004/C 281/04

European Union which call for greater security and more efficient law enforcement while protecting human rights;"

The Swedish initiative, although it was not accompanied by an impact assessment report, is perhaps the most single-minded attempt to bring substantial improvements in that field. The initiative seeks to advance cooperation by setting time limits to answer requests of information and by removing discrimination between national and intra-EU exchange of data accessible by police in at least one Member State. It is the first time since the entry into force of the Schengen Convention that an initiative intends to overhaul the general legal and operational conditions for the exchange of law enforcement data provided for in the Convention and especially in its articles 39 and 46. In its report on the initiative, the European Parliament welcomes the approach[3] and stresses the importance of ensuring the balance between the protection of fundamental rights and the extension of law enforcement competencies.

However, the initiative falls short of bringing the "innovative approach" that the Hague programme wants the Commission to adopt in the proposals that it is invited to present by the end of 2005. It contains a number of limitations to the circumstances where it applies and constitutes a traditional exchange-mechanism based on the application of the law of the requested State. The direct information exchange contacts between authorities seem appealing, but do not cater for language problems or for the respect of certain formalities. The initiative does not eliminate the unpredictability that is inherent to the application of rules alien to the requesting authorities. Furthermore, it is conceived to improve situations where the requesting law enforcement officer knows that a given Member State holds certain data, which is not often the case.

3.2. Lack of trust and confidence between law enforcement bodies

The Communication from the Commission to the Council and the European Parliament of 16 June 2004: Towards enhancing access to information by law enforcement agencies of 16 June[4], concluded that one of the factors hindering the exchange of information is the lack of trust and confidence between the different law enforcement bodies. This conclusion, based on a broad analysis of the law enforcement information exchange within the EU, revealed that the challenges resulting from that situation could be met by bringing more transparency into the process of information exchange, as well as by the introduction of the principle of equivalent access to law enforcement relevant information, that would be applicable across the board, from the access and transfer of data to their use and analysis.

However, the concept of "trust and confidence" is equally important, if not more, for civil society to accept the way their law enforcement authorities go about the management of security in the European Union. Citizens and economic operators must also trust that the gathering, exchange, use and analysis of data concerning them are done lawfully and accurately.

---

3 A6/2005/162

4 COM(2004)429 final

This situation implies, on the one hand, that all data processing must be traceable to allow for either internal or external audit or oversight, inducing lawfulness of the process and responsible behaviour, and, on the other hand, that effective legal remedies are available to citizens whose data are processed by the law enforcement body. For a citizen it should not matter in which Member State he or she wants to exercise his or her right, or which Member State is concerned. The effective remedies should also offer guarantees for the law enforcement authorities, to be able to prove the lawfulness of the data processing. The traceability of the entire process is therefore beneficial for law enforcement as well as civil society.

3.3. Technological obstacles

The aforementioned Communication of 16 June 2004 analysed the following obstacles:

- Use of diverging approaches to collect and categorise data and information.
- Differences in access privileges, user profiles and standards for the authorisation to access classified information, as well as in ways to register authorised users and their on- and offline activities with data.
- Different approaches toward electronic networking of law enforcement services.

On the basis of the work carried out in the context of the introduction of the Europol Information System, new islands of consensus on some of these aspects are likely to arise.

3.4. Obstacles linked to legal and administrative constraints

The competence to access and use data is not only linked to an appointed function in a specific organisation, but also depends on whether information is deemed to be sensitive or not. Absence of harmonisation on authorisation and classification standards causes systemic obstacles to information sharing.

3.5. Obstacles finding their origin in organisational idiosyncrasies

The comparative study carried out by the external contractor showed that systemic resistance results from organisation and operational factors which can take a number of different forms:

- Resistance to share information between authorities that below to different ministries.
- Resistance to share information obtained in the past by using coercive measures.
- Distribution of competencies over different bodies in an environment that is very much organised according to strict hierarchies, without possibilities to assess the relative competencies of the different bodies in Member States. This causes obstacles to cooperation.

3.6. Application of concepts of confidentiality and classification of information

The aforementioned Communication of 16 June 2004 analysed a number of obstacles linked to the sensitivity, confidentiality or classified nature of information:

- No single forum exists for the classification of the confidentiality of different information sources exists at this moment. Common EU standards exist for the classification of Council documents, but they have not been adapted to law enforcement use or necessities.

- Formal obligations apply when information is classified, imposing additional guarantees and the use of exclusive networks.

- The limits of source protection by police and within the context of criminal proceedings need to be embedded in procedural guarantees.

3.7. Endangered security of EU citizens

Crime, organised or otherwise, in particular terrorism, trafficking in persons and offences against children, illicit drug trafficking and illicit arms trafficking, corruption and fraud, constitute threats to citizens throughout the European Union. The institutions of the Union and the Member States must prevent and combat such crimes jointly and continuously taking into account its often trans-national nature as well new forms of threat resulting from changed economic, social and political contexts.

An efficient exchange of law enforcement relevant information between Member States has been recognized as being absolutely necessary to respond to these trans-national crimes and new forms of threat.

4. OBJECTIVES OF THE INFORMATION EXCHANGE UNDER THE PRINCIPLE OF AVAILABILTY

To meet the problems inherent to the current situation as set out above, the European Council of 4 and 5 November 2004 calls for "an innovative approach to the cross-border exchange of law-enforcement information". To introduce such approach, the Council invited the Commission to present legislation by the end of 2005 to accomplish that "with effect from 1 January 2008 the exchange of such information should be governed by [a certain number of] conditions set out [in the Hague Programme] with regard to the principle of availability, which means that, throughout the Union, a law enforcement officer in one Member State who needs information in order to perform his duties can obtain this from another Member State and that the law enforcement agency in the other Member State which holds this information will make it available for the stated purpose, taking into account the requirement of ongoing investigations in that State."

Although the Hague Programme is does not explicitly mention it, Europol should also benefit from the implementation of the principle of availability.

This Impact Assessment does not only assess whether the various options contribute to establish the intended innovative approach, but also the probable impact of those options on other public policies affected by law enforcement action.

The Hague programme, assigns the following attributes to the principle of availability:

a) the principle of availability is meant to be the fundamental operational principle for the free movement of law enforcement information throughout the European Union;

b) the principle of availability contributes to diminishing as much as possible every form of discrimination between national and intra-EU exchange of information;

c) the application of the principle of availability is prompted by the *need to have certain information in order to perform law enforcement duties*. The scope of these duties applies to the prevention, repression or investigation of criminal offences;

d) the principle of availability attributes the law enforcement authority who needs certain information a *competence to obtain* that information for the purpose for which it is needed, and an *obligation to provide* this information for the stated purpose on the holder of that information;

e) the competence and obligation resulting from the application of the principle of availability are not absolute, but are subject to a certain *conditions* that apply throughout the Union;

f) since duties of the different law enforcement authorities are not the same in all part of the Union, the principle of availability must cater for these *differences in tasks and competencies;*

g) To ensure that the principle of availability is consequential, Member States are, in principle, *obliged to know* which information is available within their national jurisdiction. This *devoir de savoir* entails not only the obligation to establish the capacity to communicate accurately whether and where the requested information is available, but also to do this quickly, i.e., in a meaningful way from a law enforcement point of view;

h) The principle of availability applies, in principle, not only to information that is held by law enforcement officials, but to all *information relevant for and accessible by law enforcement officials*, i.e. the information that officials need to perform their duties.

5. POLICY OPTIONS

On the basis of the problem analysis and the objective set out above, the responsible service defined the following four policy options.

5.1. Option 1: No legislative initiative

The first option departs from the situation where the principle of availability would not be established or no additional legislation would be considered.

However, the following developments in the current situation which have potential to contribute towards the political objectives should be noted:

- Establishment of the second generation of the Schengen Information System (SIS) with its gateway the SIRENE-bureaux. The information that is exchanged in that context is limited to the one that is explicitly foreseen in the relevant Acts of the Parliament and Council, or – in the case of SIRENE - data supporting action on the basis of SIS information. The SIS is presently conceived as a hit/no-hit control system, not to prevent or investigate criminal offences.

- Some Member States are in the process of setting up direct online access to certain national databases (Schengen II, Schengen III). These multilateral processes are taking place outside the mechanisms and cooperation structures foreseen in the Union treaties, and disregard the European dimension of law enforcement and security issues, and the interdependence of law enforcement authorities. This approach risks jeopardising the solidarity of EU Member States.

- The legislative revision of the fundamental rules on law enforcement information exchange laid down in the Articles 39 and 46 of the Schengen Convention working rules carried out by the aforementioned Swedish initiative lead to significantly improved conditions and infrastructures for law enforcement cooperation and information exchange. It intends to improve the situation *inter alia* by speeding up response times. However, it contains a number of new limitations that curb its applicability, and does neither eliminate the unpredictability inherent to such conditions nor the differentiated treatment between national and non-national requests for information. Finally, the initiative does not offer a general mechanism to support prevention and investigation of criminal offences, since it basically only allows for targeted requests of specific information known to be in the possession of the requested Member State.

- Bilateral agreements will continue to determine the information exchange landscape in order to respond to the specific needs that are not catered for by common agreement or covered in the context of a general legal framework. As it results from this enumeration, none of these instruments provides for a general and effective exchange of law enforcement relevant information from which all Member States can benefit: either because they are not conceived to prevent and investigate criminal offences or because their geographic or material scopes are limited.

5.2. Option 2: Access to information based on the principle of equivalence

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 make it inaccessible in practice. A “right of equivalent access” would make this information practically accessible to competent law enforcement authorities in the Member States under the condition of

respecting the rules that apply in the requested country. This right would imply a correspondent obligation for the requested Member State to provide information to the law enforcement authorities of another Member State that are entitled to obtain it under the law of the former.

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, and
- 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. Maintaining the division between police and judicial cooperation should therefore be ensured.

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 would be responsible for the implementation of these conditions.

The Swedish initiative mentioned above points in this direction and constitutes the first attempt to implement the principle of equivalent access on a large scale.

5.3. Option 3: Mutual recognition mitigated by a condition of equivalent access in conjunction with a mechanism to appraise the equivalence of the authorities that are competent to obtain information

The problem arising from the application of a right of equivalent access is that the conditions to meet can be different in the Member States, which hinders the full deployment of the law enforcement potential of the Union. Harmonisation would be a means to address this discrepancy.

However, the Commission does not have the intention and has not been invited to bring about such harmonisation. For that reason, mutual recognition of the competencies of the authorities in one Member State to obtain information under their national law is the best means of facilitating the information flow. Mutual recognition implies a correspondent obligation for the requested Member State to provide information to the law enforcement authorities of another Member State that are entitled to obtain it under the law of the latter.

Mutual recognition constitutes a higher level of cooperation, because of the trust and confidence that is necessary to operate the law enforcement mechanism. Because of the diversity in legal traditions and organisational idiosyncrasies in the Member

States, the straightforward application of mutual recognition will inevitably run into questions of asymmetry of competencies.

As for the proposal we submit, proposal for a Council Framework Decision on the exchange of information under the principle of availability, we have mitigated the straightforward application of the mutual recognition of competencies under national law by a common mechanism to assess the equivalence of competencies.

Nevertheless, our proposal goes further than option 3: it adds an obligation to know and to show to the obligation to provide information implied by the right of mutual recognition.

5.4. Option 4: Mutual recognition mitigated by a condition of equivalent access in conjunction with a mechanism to appraise the equivalence of the authorities that are competent to obtain information, and an index system to identify the information that is not available online

As it results from the title, option 4 actually consists of option 3 plus an additional obligation: the obligation to provide information is complemented with the obligation to know and to show which information exists within a Member State to qualify for exchange under the principle of availability. This supply each other with knowledge about available information, we propose that infrastructures are set up by Member States. In the first place to grant each other direct access to pre-determined, selected databases, allowing for direct consultation of available information. In the second place, if information can not or may not be made available online, to establish an obligation to provide index data about available information. Online consultation of these index data will tell other Member States whether solicited information is available. To be able to comply with this obligation, technical implementation is necessary in order agree on and elaborate technical architecture support. This technical support should be adapted to the nature of the data, the type of access (online or via indexation), and to the level of political ambition vis-à-vis its exchange.

We propose that the information that is identified by a matching index data, will be exchanged further to an information demand issued by the competent authority.

6. IMPACTS OF THE POLICY OPTIONS

The possible positive or negative impact of these four policy options have to be assessed, above all, with regard to the fundamental rights safeguarded by public authorities, such as the rights to life and physical integrity, on the one hand, and the rights affected by the exercise of law enforcement functions, in particular the right to the protection of personal data, on the other hand.

Regarding the fundamental rights safeguarded by public security, i.e. the protection of citizens against terrorism and serious crime, a positive impact would exist if security is likely to be improved. i.e., in terms of lives saved and physical integrity of human beings. A negative impact must stated if lives and bodies are put at risk, for example if terrorist attacks are more difficult to prevent, or to investigate.

Positive or negative effects have to be assessed regarding fundamental rights affected by public security, in particular the right to data protection i.e. the protection of the individual concerned against unjustified restrictions of his or her freedoms, in particular the right to decide him- or herself about the dissemination of own personal data. A positive impact could be stated if data protection is likely to be improved. A negative impact has to be stated if the level of data protection is likely to be reduced.

The impact assessment for the proposal for a Framework Decision on the on the protection of personal data processed in the framework of police and judicial co-operation in criminal matters also analyzes these questions in detail.

Possible financial consequences at the national level have also to be taken into account. Given the value of fundamental rights the factor "costs" seems to be of limited relevance.

6.1. Benefits and costs of Option 1: No new or additional legislation

- Fundamental rights safeguarded by public security, such as the right to life and physical integrity:

  While the present means/channels for information exchange (that, as explained in point 4.1, present important inefficiencies) would remain unchanged, the intensity of free movement of persons and concrete security threats make the information needs of enforcement authorities evolve. The increase of the information needs requires an even evolution of access to information, making it faster and easier. The absence of further development of data exchange in terms of quantity and quality amounts to loosing efficiency of judicial and police work. It seems reasonable to think that inaction would progressively lower the security level. A negative impact is therefore to be expected.

- Fundamental rights affected by public security, in particular the right to data protection:

  Inaction involves maintaining the same level of data protection and therefore no impact.

- Financial costs**:**

  No change. Obviously, no new investment is required.

6.2. Benefits and costs of Option 2: Access to information based on the principle of equivalence

- Fundamental rights safeguarded by public security, such as the right to life and physical integrity :

  Law enforcement authorities would be able to access the data stored in other Member State whenever they meet the conditions to access the data established by the latter.

  This system represents does not an improvement of the present situation, since this type of exchange of information is established and possible under Article 39 of the Schengen Implementing Convention.

Nevertheless, the system is far from being perfect as the outcome of the request is largely unpredictable. Although an obligation to answer could be set up as well as strict delays to comply with that obligation, it would be impossible for the requesting authority to know in advance whether the requested Member State would facilitate the information, as it depends on the national law of the requested Member State.

In consequence, we can predict a moderate positive effect.

- Fundamental rights affected by public security, in particular the right to data protection:

  The implementation or improvement of the principle of equivalence could amount to a slight intensification of the flow of law enforcement relevant information between Member States. Where information, including personal data, is exchanged more easily and more quickly, some individual freedoms, in particular the right to data protection, are likely to be affected to a higher degree. The risk of accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access would probably augment, especially where processing involves a transmission over a network.

  Nevertheless, the implementation of the principle of equivalence would be accompanied by the establishment of common standards on data protection, first of all, to harmonise the level of data protection in the Member States, creating the necessary confidence for the transmission of data and, secondly, to prevent the materialization of the aforementioned risks.

  Provided that these common standards correspond to options 4, 5 or 6 of the Impact Assessment for the proposal for a Framework Decision on the protection of personal data processed in the framework of police and judicial co-operation in criminal matters, they should provide for targeted rules on data processing and data protection for the exchange of information for the purpose of preventing and combating crime and, therefore, be able to ensure an appropriate data protection regime.

  These common standards on data protection especially adapted to the exchange of information for the purpose of preventing and combating crime should constitute a robust and comprehensive system covering all casualties and hindering any violation of the right to privacy and data protection resulting from the exchange of information under the principle of equivalence. They would guarantee that the data subject is generally well protected against unlawful processing of personal data.

  If, by any chance, despite the effective protection system established, any of the risks mentioned above would materialize, we must not forget that the right to life and personal integrity, which would be better protected by intensifying the flow of law enforcement relevant information, are the most valuable of human rights, without which none, or very little, of the other fundamental rights, have any meaning. Therefore, if despite the existence of a resilient and tight data protection regime, the increase of data exchange could occasionally lead to some violations of the rights to privacy and data protection, it is thought that such a result is bearable. Certainly more than the opposite situation.

- Financial costs:

  No significant costs would be involved. This mechanism of information exchange wouldn't require any further investment as the Member States wouldn't be obliged to make available data that aren't available for their own national authorities according to national law (which means there would be no need to create new data bases or files systems) and the exchange of information would take place through existing structures either Europol or central units of national authorities designated in the Member States.

  No significant impact is therefore expected.

6.3. Benefits and costs of Option 3: Access to information based on mutual recognition mitigated by a condition of equivalent access in conjunction with a mechanism to appraise the equivalence of the authorities that are competent to obtain information a mutual recognition

- Fundamental rights safeguarded by public security, such as the right to life and physical integrity :

  Mutual recognition would represent a step further in police and judicial cooperation because, in this case, law enforcement authorities would have the right to obtain information from another Member State whenever they are allowed to access that information under their own national law, eliminating the uncertainty of the previous system: law enforcement authorities would know whether they have the right to obtain certain data before asking for them. They would be operating within a quasi-familiar environment when asking for the information to another Member State, which should allow them to work in a more efficient way, amounting to a higher level of security.

  Nevertheless, that mutual recognition system is not perfect. In the first place since it implies that the legal and organisational differences between Member States are ignored. To off set that situation, we propose to include in this option a common mechanism to establish the equivalence of competencies of authorities that shall be entitled to obtain information under the principle of availability.

  In the second place, the shortcoming of mutual recognition of competencies to access information is that the results would not be completely predictable either: law enforcement authorities could ask for data they are allowed to access to find out in the end that these data are not in the possession of the requested Member State.

  Furthermore, a higher level of confidence is necessary to operate under mitigated mutual recognition and, in consequence, this possibility would necessarily be conducive of a better, more efficient, and rule-based cooperation.

  A significant positive impact can in consequence be predicted.

- Fundamental rights affected by public security, in particular the right to data protection:

  Similarly to option 2, the implementation of the right of mutual recognition would amount to intensify the flow of law enforcement relevant information between

Member States, increasing the risk of accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access would probably augment, especially where processing involves a transmission over a network.

Nevertheless, as it is the case under option 2, the implementation of the right of mutual recognition would be accompanied by the establishment of common standards on data protection and, provided that these common standards respond to options 4, 5 or 6 of the aforementioned Impact Assessment, they should provide for targeted rules on data processing and data protection for the exchange of information for the purpose of preventing and combating crime and, therefore, able to ensure an appropriate data protection regime.

These common standards on data protection specially adapted to the exchange of information for the purpose of preventing and combating crime should constitute a robust and comprehensive system covering all casualties and hindering any violation of the right to privacy and data protection resulting from the exchange of information under the right of mutual recognition. They would guarantee that the data subject is generally well protected against unlawful processing of personal data.

And, finally, if, by any chance, despite the effective protection system established, any of the risks mentioned above would materialize, the reasoning under option 2 applies.

- Financial costs:

No significant costs are involved as the Member States wouldn't be obliged to gather and store information with the sole purpose of providing it to the law enforcement authorities of other Member States (which means there would be no need to create new data bases or files systems).

As it is the case in option 3, the actual exchange of information would take place through existing structures, either Europol or central units of national authorities designated in the Member States, without involving any extra cost, and for certain categories of information only.

No significant impact is therefore expected.

6.4. Benefits and costs of Option 4: Access to information based on mutual recognition mitigated by a condition of equivalent access in conjunction with a mechanism to appraise the equivalence of the authorities that are competent to obtain information, and an index system to identify the information that is not available online

- Fundamental rights safeguarded by public security, such as the right to life and physical integrity:

This system represents an improvement of the situation under option 3 because the index system or direct access added by it simplifies and accelerates the process of obtaining information at the same time as it eliminates the risk of fishing for information that are not in the possession of the requested Member State. Either via direct automated access or via an index system, judicial and police authorities would

be able to obtain information required for the prevention, detection or investigation of criminal offences, very easily. This should amount to more efficiency in law enforcement authorities' work and, therefore, to a higher security level.

The online access to data bases or to index data would apply to targeted categories of information that are generally acknowledged to be relevant to conduct efficient law enforcement operations. So, the width of exchanges of information under this option would remain the same as under option 3.

A definitely important positive impact is expected.

- Fundamental rights affected by public security, in particular the right to data protection:

  The reasoning under option 3 applies to option 4 with the only difference that, in this case, we can speak about a concrete proposal for a Framework Decision on the protection of personal data processed in the framework of police and judicial co-operation in criminal matters that accompanies the proposal for a Framework Decision on exchange of data under the principle of availability.

  This first proposal corresponds to option 5 of the aforementioned Impact Assessment. In consequence, we can be more precise and affirm that the common standards established provide for targeted rules on data processing and data protection for the exchange of information for the purpose of preventing and combating crime in the course of activities provided for by Title VI of the Treaty on European Union and, therefore, ensure an appropriate data protection regime. They guarantee that the data subject is generally well protected against unlawful processing of personal data.

  Finally, the technical infrastructure required to operate this option will allow for traceability of all the processing of information requested, consulted or exchanged. Together with obligation to log all processing, this option offers real and significant tools for the protection of personal data, both for the data subject, as well as for supervisory authorities.

- Financial costs:

  As it is the case in option 3, there would be no obligation for the Member States to gather and store information with the sole purpose of providing it to the law enforcement authorities of other Member States. However, Member States would be obliged to know and show the information they have and the technical support required to comply with this obligation involves important expenses that they would have to face.

  Concerning the index system, they would support the costs of generating index data and developing and maintaining a National Law Enforcement Services Index System (N.LESIS) and, in the future, they could decide to connect them or bring index data together in a European Law Enforcement Services Index System (ELESIS), which would represent further costs, but which would also significantly increase law enforcement capabilities. Since the introduction of such index systems is costly, it should be agreed, in a first phase, only for information that is deemed to be extremely helpful to assist the law enforcement effort. For that reason we propose to

limit the application of the principle of availability to certain categories of information.

Concerning direct automated access, Member States would assume the costs of connecting their IT infrastructures to allow non national competent authorities to access their relevant law enforcement data.

In consequence, a considerable impact is expected. The costs would have to be better highlighted and calculated the moment that a decision on the policy option on whether (i) to grant direct access to selected categories of data or (ii) indirect access via an indexation system would be taken. This decision would obviously have important information technology consequences.

6.5. Impact summary table

The following table will show the costs and benefits of the different policy options:

	Fundamental rights protected by public Security	**Fundamental rights affected by public security, in particular data protection**	**Financial costs**
Option 1	Negative impact: progressive deterioration resulting from increasing needs of information exchange and obvious inefficiencies of present information exchange	No impact on data protection. Possible negative impact on right to life and personal integrity	No change: no new or additional investment required
Option 2	Moderate positive impact resulting from legal recognition of general exchange information system but moderate because of unpredictable outcome of the information request	Higher exposition of personal data covered, however, by an appropriate, comprehensive and robust data protection regime	No important costs
Option 3	Significant positive impact: further improvement for exchange of certain data resulting from eliminating uncertainty about right to obtain information but not about existence of information	Higher exposition of personal data covered, nevertheless, by an appropriate, comprehensive and robust data protection regime	No important costs

Option 4	Definitely important positive impact: very important improvement for exchange of certain data resulting from underpinning eliminating uncertainty via index system or direct automated access to data	Higher exposition of personal data covered, however, by an appropriate, comprehensive and robust data protection regime	Important investments from Member States are required. However, actual decision on how the duty to know and show would materialise would be taken later on.

7. COMPARISON

7.1. The table above shows that no fundamental rights would benefit from inaction. Option 1 must therefore be rejected. Between options 2, 3 and 4, the latter, access to information based on mutual recognition mitigated by a condition of equivalent access in conjunction with a mechanism to appraise the equivalence of the authorities that are competent to obtain information, and an index system to identify the information that is not available online is the most effective from the point of view of securing the right to life and physical integrity.

Concerning the impact on fundamental rights affected by public security, and data protection in particular, the three options are equivalent. As it was demonstrated above, the implementation of equivalent access or mutual recognition would be accompanied by the establishment of common standards on data protection especially adapted to the exchange of information for the purpose of preventing and combating crime. They should constitute a robust and comprehensive system ensuring that the data subject is generally well protected against unlawful processing of personal data.

If, by any chance, despite the effective protection system established, any of the risks mentioned above would materialize and extreme choices would have to be envisaged, *in dubio*, the right to life and physical integrity, without which most other fundamental rights are meaningless, should prevail. The chances of such risk are, however, significantly diminished by the existence of the envisaged third pillar data protection regime.

Considering that from the point of view of the fundamental rights safeguarded by public security, option 4 is clearly the most effective one and that, from the point of view of fundamental rights options 2, 3 and 4 are equivalent, only the financial costs could prevent us from choosing option 4., The table above shows us clearly that it is an expensive option. Nevertheless, it is by far the one expected to achieve a higher level of security. And, once more, public security and financial costs do not share equal footing: the right to life and personal integrity have such a weight that important costs should not discourage us from implementing a system when we believe it is efficient. The estimation of the cost would be done the moment the Council decision on how data should be inter-changed – either via direct access or via an indexation system – would be taken.

7.2. Impacts on society at large

The progressive establishment of an area of freedom, security and justice requires measures to align the European situation with the national one. Information exchange is crucial in this perspective. Without effective legal means at their disposal and in particular legal instruments for improving the exchange of information between law enforcement authorities of the Member States, the security (law enforcement) component of the Union will remain aback on the needs of the society.

Especially in a Union that is in need of justifying its policies to instil in society the need for more Europe, security is probably one of the issue that is most speaking to the hearts and minds of civil society, citizens and economic operators alike, irrespective of their location or of their travel throughout that territory.

7.3. Subsidiarity and proportionality

The subsidiarity principle applies insofar as police cooperation does not fall under the exclusive competence of the Community.

We consider that the objectives pursued by the implementation of the exchange of information under the principle of availability cannot be sufficiently achieved by the Member States for the following reason(s).

Common responsibility for the security of each individual Member State and for that of the Union as a whole requires a level of data exchange that meets the information needs of the law enforcement community. This level evolves with the intensity of free movement of persons throughout the EU and the concrete security threats.

Leaving the development of action to individual Member States would imply that the administration of security depends on the goodwill of third parties, thus crippling Member State's capacity to guarantee an adequate high level of security on their territory.

Union action will better achieve the objectives pursued by the implementation exchange of information under the principle of availability for the following reason(s).

The purpose of the action is to empower national law enforcement authorities and Europol officials to obtain necessary law enforcement relevant information that is accessible in one of the Member States. Without action on the level of the EU, neither the fact that information is accessible, nor the mechanisms to obtain that information could be guaranteed.

As the obstacles to obtain the information find their origin in differences in national legal and organisational idiosyncrasies, and since cooperative experience has shown that information needed for regular law enforcement tasks is available in any of the Member States, only the legislation on the level of the EU, supported by EU-wide technical infrastructure is capable of providing an approach that offers a solution to momentous security challenges.

Concerning proportionality, the purpose of the action is setting out minimum standards without hindering the development of more generous bi- or multilateral

national, Community or Union systems for information exchange and maintaining the reference to national law as a possibility where it does not hinder the efficiency and predictability of the mechanism to obtain the information.

The responsibility of Member States to organise and staff their law enforcement infrastructure finds also its expression in the financial responsibility to set up the infrastructures necessary to bring about more efficient information sharing.

7.4. Constitutional traditions of the Member States and fundamental rights

Considering the sensitiveness of the issues involved, it is important to note that the implementation of the principle of availability fully respects the constitutional traditions and values of the different Member States.

In this sense, insofar as the Charter of Fundamental Rights constitutes the common reflection of the values protected by the constitutions of all Member States, it should be emphasised that the aim of the action is to contribute to the implementation of Article 2 and 3 of the Charter of Fundamental Rights which states that everyone has the right to life and physical integrity.

Furthermore, the implementation of the principle of availability respects Article 6 TEU that puts the respect for human rights and fundamental freedoms at the centre of the activities of the Union. It does this by promoting cross border information exchange in keeping with the fundamental rights and principles recognised by the Charter and Article 6 TEU. Moreover, the processing of data is protected in accordance with Article 8 of the Charter.

7.5. Conclusions

7.6. Therefore, the Commission recommends option 4, acess to information based on mutual recognition mitigated by a condition of equivalent access in conjunction with a mechanism to appraise the equivalence of the authorities that are competent to obtain information, and an index system to identify the information that is not available online.

8. MONITORING AND EVALUATION

With regard to the implementation of the proposed option, i.e. a Framework Decision on exchange of information under the principle of availability by Member States, it shall be evaluated in accordance with the usual procedures under Title VI of the Treaty on European Union. Member States shall transmit to the General Secretariat of the Council and to the Commission the text of the provisions transposing into their national law the obligations imposed on them under this Framework Decision. On the basis of this information and a written report from the Commission, the Council shall before December 2008 assess the extent to which Member States have taken the measures necessary to comply with this Framework Decision, and take all measures necessary to ensure its full application.

Once the provisions transposing into national law the obligations imposed under this Framework Decision have been adopted by Member States, the efficiency of the system could be measured by using the following indicators:

1. Number of information exchanges between competent authorities under the Framework Decision, in particular:

   (a) Number of requests sent by each Member State

   (b) Number of positive answers received by each Member State

2. Average delay of information exchange under the Framework Decision (from the formulation of the request to the reception of the answer).

3. Number of solved cases in which information exchange under the Framework Decision intervened at a certain stage.

   This data should be collected annually by the competent authorities and transmitted to the Commission, which could note the progress made in a year basis.