COMMISSION OF THE EUROPEAN COMMUNITIES

Brussels, 4.10.2005
SEC(2005) 1241

COMMISSION STAFF WORKING DOCUMENT

Annex to the:

Proposal for a Council Framework Decision on the protection of personal data processed in the framework of police and judicial co-operation in criminal matters

IMPACT ASSESSMENT

{COM(2005) 475 final}

TABLE OF CONTENTS

1. Procedural issues and consultation of interested parties 5
1.1. Governments of Member States and of Iceland, Norway and Switzerland 5
1.2. Independent data protection authorities 6
1.3. European Parliament 6
1.4. Results 6
2. Problems in the current situation 7
2.1. Endangered security of EU citizens 7
2.2. Availability of information needed to provide security for EU citizens 7
2.3. Risks for fundamental rights, in particular for the right to data protection 8
2.4. Competence to act and subsidiarity 9
3. objectives and orientation set out by the Council 10
3.1. Objectives 10
3.1.1. Providing security for EU citizens by improving the exchange of information 10
3.1.2. Ensuring data quality 10
3.1.3. Respecting fundamental rights 11
3.2. Orientations set out by the Council 12
3.3. Objectives in the light of the principle of availability 12
3.4. Consistency with other instruments regarding data protection 13
4. Policy Options 14
4.1. Option 1: No legislative initiative 14
4.2. Option 2: Application of Directive 95/46/EC 15
4.3. Option 3: Legislative initiative once the modalities for the exchange of information under the principle of availability have been defined 16
4.4. Option 4: Specific provisions in a legal instrument on the exchange of information under the principle of availability 17
4.5. Option 5: Framework Decision on common standards for the processing and protection of personal data in the course of activities provided for by Title VI of the Treaty on European Union 17
4.6. Option 6: Legislative initiative involving all existing EU information systems or bodies (Europol, Eurojust) 18
5. impacts of the policy options 18
5.1. Benefits and costs of Option 1: No legislative initiative 19
5.1.1. Respect for fundamental rights safeguarded by public security, in particular the right to life and physical integrity 19
5.1.2. Respect of fundamental rights affected by public security, in particular the right to data protection 20

5.1.3. Consistency of the Union's data protection policy 20
5.1.4. Costs 20
5.2. Benefits and costs of Option 2: Application of Directive 95/46/EC 20
5.2.1. Respect for fundamental rights safeguarded by public security, in particular the right to life and physical integrity 20
5.2.2. Respect of fundamental rights affected by public security, in particular the right to data protection 20
5.2.3. Consistency of the Union's data protection policy 21
5.2.4. Costs 21
5.3. Benefits and costs of Option 3: Legislative initiative once the modalities for the exchange of information under the principle of availability have been defined 21
5.3.1. Respect for fundamental rights safeguarded by public security, in particular the right to life and physical integrity 21
5.3.2. Respect of fundamental rights affected by public security, in particular the right to data protection 21
5.3.3. Consistency of the Union's data protection policy 21
5.3.4. Costs 21
5.4. Benefits and costs of Option 4: Specific provisions in a legal instrument on the exchange of information under the principle of availability 22
5.4.1. Public security and 22
5.4.2. Respect of fundamental rights, in particular the right to data protection 22
5.4.3. Consistency of the Union's data protection policy 22
5.4.4. Costs 22
5.5. Benefits and costs of Option 5: Framework Decision on common standards for the processing and protection in the course of activities provided for by Title VI of the Treaty on European Union 22
5.5.1. Respect for fundamental rights safeguarded by public security, in particular the right to life and physical integrity 22
5.5.2. Respect of fundamental rights affected by public security, in particular the right to data protection 22
5.5.3. Consistency of the Union's data protection policy 23
5.5.4. Costs 23
5.6. Benefits and costs of Option 6: Legislative initiative involving all existing EU information systems or bodies 23
5.6.1. Respect for fundamental rights safeguarded by public security, in particular the right to life and physical integrity 23
5.6.2. Respect of fundamental rights affected by public security, in particular the right to data protection 23
5.6.3. Consistency of the Union's data protection policy 23

5.6.4. Costs....24
5.7. Impact summary table....24
6. Comparing the options....26
7. Monitoring and Evaluation....26

Executive summary

The security for citizens in the European Union and its Member States has acquired a new urgency, especially in the light of the terrorist attacks in the United States on 11 September 2001, in Madrid on 11 March 2004 and in London on 7 July 2005. Against this background the European Council, in The Hague Programme on strengthening freedom, security and justice, invited the Commission to submit proposals for the implementation of the principle of availability, in which key conditions in the area of data protection should be strictly observed. In its Declaration of 13 July 2005 on the EU response to the London bombings the Council (Justice and Home Affairs), inter alia, calls on the Commission to present these proposals by October 2005.

The principle of availability means that, throughout the Union, a law enforcement officer in one Member State who needs information, including personal data, 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. Consequently, the introduction of this principle will affect the right to data protection and has to be accompanied and counterbalanced by appropriate legal provisions.

The Commission consulted the Governments and the independent data protection authorities of the Member States and of Iceland, Norway and Switzerland, the European Data Protection Supervisor; Europol and Eurojust. The Commission took into consideration the positions expressed by the European Parliament and at the 2005 Spring Conference of the European Data Protection Authorities.

The Commission considered six different options in order to provide for an appropriate legal regime for data processing and protection in the course of police and judicial cooperation in criminal matters: (1) no legislative initiative; (2) application of Directive 95/46/EC; (3) legislative initiative once the modalities for the exchange of information under the principle of availability have been defined; (4) specific provisions in a legal instrument on the exchange of information under the principle of availability; (5) Framework Decision on common standards for the processing and protection of personal data in the course of activities provided for by Title VI of the Treaty on European Union; (6) legislative initiative involving all existing EU information systems or bodies.

The Commission assessed the impact of these options on public security, fundamental rights, in particular the right to data protection, the consistency of the Union's data protection policy and costs. The Commission recommends option 5 given its positive impacts in all these areas and the need to implement by January 2008 the principle of availability while maintaining a high level of data protection.

1. PROCEDURAL ISSUES AND CONSULTATION OF INTERESTED PARTIES

1.1. Governments of Member States and of Iceland, Norway and Switzerland

On 22 November 2004 and on 21 June 2005, the Commission invited and consulted experts representing the Governments of Member States and of Iceland, Norway and Switzerland.

1.2. Independent data protection authorities

On 11 January 2005, the Commission convened a consultative meeting with the Data Protection Authorities of these States. The European Data Protection Supervisor, Europol, Eurojust, and the Secretariat of the Joint Supervisory Bodies were involved. The Working Party set up according to Article 29 of Directive 95/46/EC was regularly informed about the ongoing development.

The Commission took into account the results of the Spring Conference of the European Data Protection Authorities, Krakow, 25-26 April 2005,

On 12 April and 21 June 2005, the Commission attended meetings of the Police Working Party of the Conference of the European Data Protection Authorities.

1.3. European Parliament

On 31 January 2005, the Commission participated in a "Public Seminar: Data protection and citizens' security: what principles for the European Union?" held by the Committee on Civil Liberties, Justice and Home Affairs. The Commission took into account the position of the European Parliament as set out, inter alia, in the European Parliament recommendation to the European Council and the Council on the exchange of information and cooperation concerning terrorist offences (2005/2046(INI)), adopted on 7 June 2005.

1.4. Results

The main purpose of the consultations was to find out the need for a legal instrument on the processing and protection of personal data in the third pillar and, if so, what the main content of such an instrument should be. The Commission asked representatives of the Governments of the Member States and of the Schengen States as well as the representatives of the Data Protection Authorities of these States, inter alia on the basis of a questionnaire and a discussion paper, about their position concerning the general approach of a new legal instrument and its relation to existing instruments, the legal basis, the possible scope, the principles relating to data quality, the criteria for making data processing by police or judicial authorities legitimate, personal data of non-suspects, the requirements for the transmission of personal data to competent authorities in other Member States and in third countries, the rights of the data subject, supervisory authorities and a possible advisory body for data protection in the third pillar.

Both the European Parliament and the Data Protection Authorities in the European Union strongly support a legal instrument providing for common standards for the processing and the protection of personal data in the third pillar. Representatives of the Governments of the Member States and of Iceland, Norway and Switzerland, furthermore of Europol and Eurojust did not express a common position in that regard. But the Commission could conclude that there was no fundamental opposition to the idea of such an instrument provided it would have an added value at EU level taking into account the necessity of data protection provisions that are consistent with the purpose for which information is processed. There seemed to be agreement that the implementation of the principle of availability has to be accompanied by appropriate counterbalancing rules in the area of data protection. In that context, some Member States stated that the way information is exchanged in the future should be defined first and that rules for the processing and protection of personal data should be laid down subsequently. Some preferred a set of specific provisions to be included in the act on the principle of availability.

2. PROBLEMS IN THE CURRENT SITUATION

2.1. 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, constitutes a threat to citizens throughout the European Union. The institutions of the Union and the Member States have a special role in preventing and combating such crime 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.

The security for citizens in the European Union and its Member States has acquired a new urgency, especially in the light of the terrorist attacks in the United States on 11 September 2001, in Madrid on 11 March 2004 and in London on 7 July 2005. *The Hague Programme on Strengthening, Freedom, Security and Justice in the European Union*,[1] adopted by the European Council on 4 November 2004, points out that the citizens of Europe rightly expect the European Union, while guaranteeing respect for fundamental freedoms and rights, to take a more effective, joint approach to cross-border problems such as illegal migration, trafficking in and smuggling of human beings, terrorism and organised crime, as well as the prevention thereof. Notably in the field of security, the coordination and coherence between the internal and the external dimension has been growing in importance and needs to continue to be vigorously pursued.

2.2. Availability of information needed to provide security for EU citizens

The Hague Programme states that strengthening freedom, security and justice requires an innovative approach to the cross-border exchange of law enforcement information. The mere fact that information crosses borders should no longer be relevant. The underlying assumption is that serious crimes, in particular terrorist attacks, could be better prevented or combated if the information gathered by law enforcement authorities in EU Member States would be more easily, more quickly and more directly available for the law enforcement authorities in all other Member States.

With effect from 1 January 2008 the exchange of such information should be governed by 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.

In The Hague Programme *the Commission is invited to submit proposals* by the end of 2005 at the latest *for implementation of the principle of availability*, in which key conditions in the area of data protection should be strictly observed. In its *Declaration of 13 July 2005 on the EU response to the London bombings* the Council (Justice and Home Affairs), inter alia, calls on the Commission to present proposals on data protection principles in the field of law enforcement and, in accordance with the Hague programme, on the principle of availability by *October 2005*.

---

[1] OJ C 53, 3.3.2005, p. 1

The introduction of the exchange of information under the principle of availability has to be seen in a wider context. Firstly, the Commission proposes a Framework Decision on the exchange of information under the principle of availability. That proposal shall lay down the basic rights and obligations of the Member States under the principle of availability. In the near future, the Commission will submit proposals for legal instruments on mutual consultation of DNA databases and on the improved exchange of fingerprint data that shall be consistent with the principle of availability.

2.3. Risks for fundamental rights, in particular for the right to data protection

Police and judicial cooperation in criminal matters implies that very personal, possibly intimidating, information about individuals (personal data) is collected, stored and transmitted, in many cases even where the individuals concerned are not suspected of intending to commit or of having committed a criminal offence (e.g. victims, witnesses, relatives, friends, neighbours or other contact persons of the suspects). Substantial interests of individuals are concerned and information revealing details about them and their life must only be processed if necessary for a legitimate purpose laid down by law. This requirement is recognised in Article 8 of the EU Charter for Fundamental Rights, which contains the right of everybody to the protection of personal data concerning him or her. Furthermore, the right to data protection follows from the European Convention for the Protection of Human Rights and Fundamental Freedoms and is the subject of Convention No 108 of 1981 for the Protection of Individuals with regard to Automatic Processing of Personal Data. Any step enhancing and intensifying the exchange of information in the course of police and judicial cooperation in criminal matters must respect the right to data protection.

Taking into account the principle of proportionality, the balance has to be struck between the necessity of efficiently exchanging personal data in order to prevent and combat crime, in particular terrorism and serious organised crime, and the right of the individual to data protection. Any person could be affected. A well balanced approach is crucial for

- the public, i.e. individuals who shall be protected against crime, in particular terrorism and serious organised crime,
- police and judicial authorities which should be able to efficiently fulfil their legitimate tasks in order to guarantee the protection referred to in the first indent,
- individuals whose personal data may be processed by police and judicial authorities for the reasons set out above.

The introduction of the principle of availability will fundamentally change the exchange of information, including personal data, in the area of police and judicial cooperation in criminal matters. Under the principle of availability information shall be exchanged more easily, more quickly and more directly between the competent authorities of the Member States. Such development will contribute to reducing the time an authority needs to collect information that is necessary in the course of a particular investigation.

Where information, including personal data, is exchanged more easily, more quickly, more directly and, probably, more often, individual freedoms, in particular the right to data protection, will be affected to a higher degree. The risk resulting from – although most probably unintended - non-compliance with fundamental data

protection principles and, consequently, the risk for the individual concerned of suffering financial or immaterial damages caused by the exchange of incorrect, inaccurate or non up-dated information is likely to increase. Besides, the latter does not only affect the rights of the individual concerned but also the quality of the work carried out by the competent authorities. Where personal data are more easily available for the authorities in all Member States, the quality of these data becomes even more important. Incorrect, inaccurate or outdated data hold the potential of damaging police and judicial activities throughout the Union.

In The Hague Programme the European Council underlined the necessity of guaranteeing respect for fundamental freedoms and rights. In particular, with regard to the exchange of information under the principle of availability it is stressed that key conditions in the area of data protection must be strictly observed.

Moreover, on 25 and 26 April 2005 the *European Data Protection Authorities* at their Spring Conference in Krakow adopted a declaration in which they recognized the need for closer co-operation between law enforcement authorities, within the EU and with third States. They added, however, that given the Union's obligation to respect human rights and fundamental freedoms, initiatives to improve law enforcement in the EU, such as the availability principle, should only be introduced on the basis of an *adequate system of data protection arrangements* guaranteeing a high and equivalent standard of data protection.

Finally, taking into account current activities aimed at improving the exchange of information for the purpose of preventing and combating crime the *European Parliament* in its recommendation to the European Council and the Council on the exchange of information and cooperation concerning terrorist offences (2005/2046(INI)), adopted on 7 June 2005, recommended harmonising existing rules on the protection of personal data in the instruments of the current third pillar, bringing them together in a single instrument that guarantees the same level of data protection as provided for under the first pillar.[2]

2.4. Competence to act and subsidiarity

The Union has a right to act in according to Articles 30, 31 and 34 (2) (b) of the Treaty on European Union. In the light of the implementation of the principle of availability, appropriate provisions regarding the processing and protection of personal data, including common standards for the transmission of personal data to third countries and international bodies, are essential to improve police and judicial cooperation criminal matters, in particular for the fight against terrorism and serious crimes. Moreover, Member States will only fully trust each other if there are clear and common rules for the possible further transmission of exchanged data to other parties, in particular in third countries.

The problems described above affect police and judicial cooperation in criminal matters between the Member States, in particular the exchange of information in order to ensure and promote efficient and lawful measures to prevent and combat crime, especially serious crime and terrorism. National, bilateral or multilateral solutions might be helpful for individual Member States but would disregard the necessity of ensuring internal security for the whole Union. The approximation of

---

[2] No. 1 h of European Parliament recommendation to the European Council and the Council on the exchange of information and cooperation concerning terrorist offences (2005/2046(INI)), adopted on 7 June 2005

relevant laws and regulations cannot be done adequately by the Member States acting unilaterally and requires concerted action in the European Union. Therefore, common action in order to solve the above problems respect the principle of subsidiarity provided for by Article 2 of the Treaty on European Union and Article 5 of the Treaty establishing the European Community. Furthermore, in accordance with the principle of proportionality, as set out in the latter Article, any proposed option to overcome the above mentioned problems shall not go beyond what is necessary in order to achieve that objective. Rules on data processing and protection can only be established if they are necessary to foster police and judicial cooperation in criminal matters, i.e. to allow proper and legitimate exchange of information, including personal data in full respect of the right to data protection.

3. OBJECTIVES AND ORIENTATION SET OUT BY THE COUNCIL

3.1. Objectives

3.1.1. Providing security for EU citizens by improving the exchange of information

One of the major objectives pursued with this initiative is *providing citizens with a high level of safety within an area of freedom, security and justice*. EU citizens must be protected in the best possible way against crime, especially terrorist attacks and other serious offences of trans-national nature. The Union has to develop *common action among the Member States in the fields of police and judicial cooperation in criminal matters* as set out in Article 2, fourth indent, and, more precisely, in Title VI of the Treaty on European Union. Such cooperation must be efficient and successful and requires, in particular, *improving the exchange of relevant information, including personal data*, between the competent authorities of the Member States in order to prevent and combat terrorism and other forms of serious crime throughout the Union. The European Union must provide for the *appropriate legal framework* and, where suitable, promote technical solutions that ensure such an exchange of information, including personal data, and facilitate further operational cooperation.

3.1.2. Ensuring data quality

The efficiency of police and judicial cooperation in criminal matters does not only depend on the speed and rapidity, in which information is exchanged, nor is it necessarily a matter of quantity. However, success in preventing and combating crime does always rely on the *quality* of exchanged information. Only information, which is correct, accurate and up-dated, will finally be helpful for the competent police and judicial authorities – information which does not comply with quality criteria holds the risk of resulting in misled operations and is contra productive. Consequently, the quality of data must be ensured by *appropriate obligations of the competent authorities*, in particular if data are made available to others. In addition to such obligations, the *rights of the data subject* and the *powers of independent supervisory authorities* are also extremely important to ensure data quality. Exercising these rights and powers can result in deletion or rectification of incorrect, inaccurate or outdated data and prevent the competent authorities from wasting their time due to misinformation. *At EU level regular exchange of experience of the independent supervisory authorities* is likely to have a supplementary positive effect on ensuring data quality.

The data controller's responsibility for data quality and for compliance with relevant data protection rules is particularly important when data are transmitted to another party. It can happen that the data controller has to delete or rectify data that were

made available to others. In such cases the interests of the recipient as well as of the data subject are affected. The recipient will usually consider the information as correct, accurate and updated as long as nothing to the contrary has been communicated; but data, which are no longer correct, accurate and updated, can prejudice the investigations of the recipient. The data subject, on the other hand, has an interest that personal data concerning him/her, that had to be deleted or rectified, do not continue to exist or to be inaccurate elsewhere. Otherwise, the data subject might be confronted in another Member State with disadvantages the deletion or rectification intended to avoid. The data controller can easily prevent such negative consequences by informing the recipient of any change of the data quality resulting in deletion or rectification after the transmission. Appropriate *obligations to inform the recipient* are useful and necessary.

3.1.3. Respecting fundamental rights

As set out in Article 6 of the Treaty on European Union, the Union is founded on the *principles of liberty, democracy, respect for human rights and fundamental freedoms, and the rule of law.* It shall respect fundamental rights, as guaranteed by the European Convention for the Protection of Human Rights and Fundamental Freedoms (ECHR) signed in Rome on 4 November 1950 and as they result from the constitutional traditions common to the Member States. In the context of the processing of personal data the *right to the respect for privacy* as set out in Article 8 of the ECHR and the *right to data protection* as set out in Article 8 of the Charter of Fundamental Rights of the European Union are particularly important. In principle, everybody has the right to decide him- or herself about the collection, storage and further processing as well as the dissemination of information concerning him or her. Legislation and other measures that aim at improving the exchange of information according to Title VI of the Treaty on European Union must strictly observe these rights and exactly define the conditions under which the right of the individual to privacy and to data protection can be restricted for reasons of public security. Clear definitions are necessary for the conditions under which information concerning an individual can be collected, stored, further processed and, in particular, transmitted to third parties.

Especially the transmission of personal data to others and their further processing by the recipient usually affect the rights of the data subject and, at the same time, the interest of the transmitting authority (data controller). The latter is obliged to the data subject to respect data protection principles, when processing personal data, including the transmission to the authorities of other Member States. The data controller should only transmit personal data to another Member State, if it is sure that also the latter will respect the said principles and obligations, when further processing the received data, e.g. when further transmitting them to third countries. Otherwise, the data controller violates its obligations to the data subject. The recipient should be legally obliged to respect the same rules and obligations to the data subject, which the data controller has to observe. In view of an EU wide exchange of information under the principle of availability, appropriate rules are necessary concerning the further processing of transmitted data, e.g. in order to ensure that the recipient will not make available data to third countries more easily than the data controller. Some guidance is provided by Principle 5 of Recommendation R (87) 15, which concerns the communication of personal data within the police sector, to other public bodies, to private parties as well as

international communication. Legally binding provisions, however, do not exist either within the Council of Europe or at the level of the European Union.

3.2. Orientations set out by the Council

In The Hague Programme the European Council has stressed that the mere fact that information crosses borders should no longer be relevant under the principle of availability. The methods of exchange of information should make full use of new technology and must be adapted to each type of information, where appropriate, through reciprocal access to or interoperability of national databases, or direct (on-line) access, including for Europol, to existing central EU databases such as the SIS.

The Hague Programme stresses that the following key conditions in the area of data protection should be strictly observed in the proposals the Commission shall submit:

- the exchange may only take place in order that legal tasks may be performed;
- the integrity of the data to be exchanged must be guaranteed;
- the need to protect sources of information and to secure the confidentiality of the data at all stages of the exchange, and subsequently
- common standards for access to the data and common technical standards must be applied;
- supervision of respect for data protection, and appropriate control prior to and after the exchange must be ensured;
- individuals must be protected from abuse of data and have the right to seek correction of incorrect data.

Moreover, common standards for the processing and protection of personal data in the third pillar were already discussed in 1998. On 3 December 1998, the Council (Justice and Home Affairs) adopted the Action Plan of the Council and the Commission on how best to implement the provisions of the Treaty of Amsterdam on an area of freedom, security and justice.[3] The plan stipulated that - with regard to horizontal problems in the context of police and judicial cooperation in criminal matters - the possibilities for harmonised rules on data protection should be examined within two years from the entry into force of the Treaty. In 2001, first efforts ended without success when no agreement could be achieved on a Draft Resolution on the personal data protection rules in instruments under the third pillar of the European Union.[4] In principle, however, the Action Plan shows the Council's positive and open approach towards harmonised rules on data protection in the third pillar.

3.3. Objectives in the light of the principle of availability

With regard to the objectives to be achieved it has to be taken into account that the Commission submits a proposal for Framework Decision on the exchange of information under the principle of availability. Its core element is a right for the competent authorities of one Member State to obtain information existing in another Member State in order to prevent, detect or investigate criminal offences, in particular serious and organised crime, terrorist acts and threats. This right corresponds with an obligation of the other Member State to make the information

---

3 OJ C 19, 23.1.1999, p. 1

4 Council Working Document 6316/2/01 REV 2 JAI 13

available. The principle of availability means a system of mutual rights and obligations aimed at the exchange of information. Such a system implies the processing, especially the exchange of personal data and has an impact on the fundamental rights of the data subject. Therefore, the implementation of such a system requires rules on the processing and protection of personal data that, on the one hand, support the exchange of information under the principle of availability and, on the other hand, ensure the respect of the fundamental principles of data processing and data protection as set out above.

3.4. Consistency with other instruments regarding data protection

Provisions concerning data protection do already exist at EU level. The Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data[5] contains fundamental rules on the lawfulness of the processing of personal data as well as the rights of the data subject. It includes provisions concerning judicial remedies, liability and sanctions, the transfer of personal data to third countries, codes of conduct, a specific supervisory authority and working party and finally community implementing rules. But Directive 95/46/EC does not apply to the processing of personal data in the course of activities provided for under Title VI of the Treaty on European Union.

The protection of personal data is addressed in those instruments adopted under Title VI of the TEU that organise the exchange of information between police, customs and judicial authorities of Member States through common information systems or police or judicial bodies established at European level, such as: the Convention implementing the Schengen Agreement of 1990 including specific data protection provisions applicable to the Schengen Information System;[6] the Europol Convention of 1995[7] and, inter alia, the Rules governing the transmission of personal data by Europol to third States and third bodies;[8] the Decision setting up Eurojust of 2002[9] and the Rules of procedure on the processing and protection of personal data at Eurojust;[10] the Convention on the use of information technology for customs purposes of 1995, including personal data protection provisions applicable to the Customs Information System;[11] furthermore the Convention on Mutual Assistance in Criminal Matters between the Member States of the European Union of 2000, in particular Article 23.[12] With regard to Schengen Information System particular attention has to be paid to the establishment, operation and use of the second generation Schengen information system (SIS II), for which the Commission already submitted proposals for a Council Decision[13] and for two Regulations.[14] However, where personal data are exchanged in the course of police and judicial cooperation in criminal matters without using one of the said information systems or bodies the third pillar instruments mentioned above do not apply.

---

5 OJ L 281, 23.11.1995, p. 31
6 OJ L 239 , 22.9.2000, p. 19
7 OJ C 316, 27.11.1995, p. 2
8 OJ C 88, 30.3.1999, p. 1
9 OJ L 63, 6.3.2002, p. 1
10 OJ C 68, 19.3.2005, p.1
11 OJ C 316, 27.11.1995, p. 34
12 OJ C 197, 12.7.2000, p. 1, 15
13 COM (2005) 230 final
14 COM (2005) 236 final, COM (2005) 237 final

The above mentioned instruments do not apply to the *direct* exchange of information between the competent authorities of the Member States in the context of police and judicial cooperation in criminal matters, but they include a number of provisions on relevant issues. These issues have also to be addressed regarding the direct exchange of information within police and judicial cooperation in criminal matters (e.g. principles relating to data quality, information to be given to the data subject, right of access, confidentiality and security of processing, advisory bodies etc.). If a new legal instrument should be proposed and adopted under Title VI of the Treaty on European Union, it has be consistent with existing ones in both the first and the third pillar.

Furthermore, attention has to be paid to the Council of Europe Convention No. 108 for the Protection of Individuals with regard to Automatic Processing of Personal Data of 1981 (Data Protection Convention), to its Additional Protocol of 2001 regarding supervisory authorities and transborder data flows and to the Recommendation No R (87) 15 of 1987 regulating the use of personal data in the police sector. All Member States are parties to the Convention, not all Member States are parties to the Additional Protocol.

4. POLICY OPTIONS

On the basis of the problem analysis and in view of the implementation of the principle of availability, the Commission considered the following policy options in order to achieve the objectives set out in chapter 3.

4.1. Option 1: No legislative initiative

The option of rejecting any legislative initiative could refer to existing legal instruments, in particular to Directive 95/46/EC and to the Data Protection Convention of the Council of Europe.

However, Directive 95/46/EC does not apply to the processing of personal data in the third pillar. Even the disappearance of the pillar architecture would not automatically result in the application of the Directive. Its Article 3 does not only clearly say that it shall not apply to processing of personal data in the course of an activity which falls outside the scope of Community law, such as those provided for by Titles V and VI of the Treaty on European Union. It also explicitly excludes the applicability of the Directive *in any case* for processing operations concerning *public security*, defence, State security (including the economic well-being of the State when the processing operation relates to State security matters) and the *activities of the State in areas of criminal law.* Nevertheless, it has been stressed, in particular by the Data Protection Authorities, that the majority of Member States stated that they apply the Directive to the activities of police, customs, judicial and other competent authorities concerned with the prevention of and the fight against crime.

So far, data protection provisions existing at the national level on the basis of the Directive and the Council of Europe instruments did not, at least not considerably, hamper the exchange of information between the competent authorities of the Member States. There are no clear indications that the efficiency of police and judicial cooperation in criminal matters and, finally, public security could be endangered by existing provisions on data processing and protection. In general, Member States provide for a legal framework on data protection enabling them to exchange information with other Member States. At the national level there are provisions setting out the relevant obligations of the competent authorities with

regard to data quality principles and criteria for the lawfulness of data processing, the rights of the data subject and the role of independent supervisory authorities although there are legal and practical differences. Furthermore, the Data Protection Authorities refer to the *high level of data protection provided for by the Directive* and stress that such standard should also be guaranteed in the area of police and judicial cooperation in criminal matters. Such a standard on the basis of the Directive is very likely to promote the respect of fundamental rights, in particular the right to data protection.

On the other hand, Directive 95/46/EC and the Data Protection *Convention* do not contain precise rules for data processing in the course of police and judicial cooperation in criminal matters. *Recommendation No R (87)*, on the other hand, although more specific and of huge relevance, is finally a *non-binding instrument*.

In view of the implementation of the principle of availability the existing legal regime on data protection could be problematic. Account must be taken of the at least theoretical possibility in some Member States of refusing the transmission of personal data for reasons connected with the level of data in the requesting state. Moreover, there is a need for more precise rules for the transmission of personal data to law enforcement authorities of other Member States, for the rights of the data subject and for a model providing for independent advice from data protection authorities at EU level. Insofar it might be helpful to compare the existing legal regime on data protection with usual bi- or multilateral agreements concerning the exchange of information for the purpose of preventing and combating crime. In general, such agreements seem to contain much more precise rules about the further processing, especially the further use, of data that are transmitted to another party as well as about more specific obligations of the data controller before or after a transmission. To some extent such rules do also exist in current instruments on the exchange of information through European central data bases (SIS, CIS) or bodies (Europol, Eurojust). A similar level of preciseness should be reached for the direct exchange of information between the competent authorities of Member States as well. The principle of availability establishes a comprehensive system of mutual rights and obligations for the exchange of information (so far the subject of bi- or multilateral agreements). Existing provisions on data processing could possibly prejudice such approach and seem to not provide for clear rules governing all aspects of data processing and protection that could be relevant for the exchange of information within police and judicial cooperation in criminal matters.

4.2. Option 2: Application of Directive 95/46/EC

Another option to be considered is providing for the applicability the Directive 95/46/EC to data processing for the purpose of preventing and combating crime. This option is very close to the first one. Practically, it means transposing the provisions of the Directive (first pillar instrument) into a Framework Decision (third pillar instrument) without any or only slight modifications. Again it has to be recognised that most Member States are said to apply the Directive, irrespective of its Article 3, also to data processing for the purpose of preventing and combating crime. However, those Member States benefit from wide exceptions provided for by Article 13 of the Directive and thus from a wide room for discretion.

The inapplicability of the Directive is not just a formal question linked to the pillar architecture but follows from the fact that the Directive was adopted for very different purposes. The basic principles of data processing and data protection are the same in the first and in the third pillar. But the Directive does not specifically address

data processing and data protection in the context of preventing and combating crime. For example, the criteria set out in Article 7 for making data processing legitimate may be interpreted in a way that allows applying them to preventing and combating crime. But they do not take into account more specific conditions that should apply in this context. More specific rules are only laid down in the principles of Recommendation R (87) 15, which is a non binding instrument.

Finally, arguments raising doubts about option 1 are also relevant for option 2.

4.3. Option 3: Legislative initiative once the modalities for the exchange of information under the principle of availability have been defined

The Commission also considered submitting, as a first step, a proposal defining the modalities of exchanging information under the principle of availability and developing appropriate data protection rules as a second step. This option might refer to the Council (Justice and Home Affairs) on 14 April 2005 in Luxembourg as a starting point. In fact, the Council agreed on a gradual approach to the implementation of the principle of availability consisting of the selection of six types of information considered important for criminal investigations (DNA, fingerprints, ballistics, vehicle registrations, telephone numbers, minimum data for identification of persons as contained in civil registers) and the determination of the most suitable modalities for implementing the principle of availability (indirect access to information upon request, direct access to data bases of another Member State, indirect access to information of another Member State through a central index, enhanced access to police data rendered public by Member States' law enforcement authorities). In principle, it is possible to firstly determine the right modalities for the various types of information and to subsequently define the necessary supplementary rules for data processing and protection. Such approach stresses that data protection provisions can only be developed in view of a very specific purpose, a specific modality of the exchange of information and of a specific type of information.

On the other hand, this approach holds the risk of achieving agreement on (technical) modalities for the exchange of specific types of information (e.g. DNA, fingerprints) without reaching consensus on *sufficient* supplementary provisions on data processing and data protection. The right to data protection might be at risk in this case. It should be recalled that the exchange of information according to the Schengen cooperation only started on the basis of agreed safeguards for data protection. Option 3 might also be contrary to the approach favoured in the Action Plan of the Council and the Commission on how best to implement the provisions of the Treaty of Amsterdam on an area of freedom, security and justice. The Action Plan underlines the interest of the Council in the possibilities for harmonised rules on data protection with regard to horizontal problems in the context of police and judicial cooperation in criminal matters. Another risk resulting from option 3 could be the temporary inapplicability of the modalities agreed upon for the exchange of information under the principle of availability due to the fact that sufficient data protection provisions are not yet in force.

In general, the modalities referred to by the Council on 14 April 2005 for implementing the principle of availability concern the exchange of information without using a European centralised information system or a European body such as the Schengen Information System, the Customs Information System, Europol and Eurojust. With regard to data processing and data protection *all* these modalities require rules:

- ensuring the quality of data that could be transmitted to police or judicial authorities of other Member States,
- providing for safeguards regarding the further processing of personal data transmitted to police or judicial authorities of other Member States, especially regarding their further transmission to third countries,
- ensuring the right of the individual concerned to data protection,
- ensuring necessary control of compliance with relevant standards by independent supervisory authorities.

Consequently, fundamental data protection principles can be established and apply to all the said modalities. Where necessary, they can be supplemented by more specific provisions for individual modalities of the exchange of information or the types of information that are exchanged. At the end there are no convincing reasons to wait with the development of appropriate data protection provisions.

4.4. Option 4: Specific provisions in a legal instrument on the exchange of information under the principle of availability

A fourth option could be a set of provisions on data processing and protection to be included in a legal instrument on the exchange of information under the principle of availability. Option 4 could be based on the reasons supporting option 3 while avoiding possible disadvantages (time factor). A closer link between provisions defining the modalities of exchanging information under the principle of availability and appropriate provisions on data processing and protection could possibly be established. Both types of provisions would be negotiated and adopted by the Council at the same time. Finally, a well balanced chapter on data processing and protection within a legal act on the exchange of information under the principle of availability could probably foster police and judicial cooperation in criminal matters as well as promote proper respect for fundamental rights.

On the other hand, choosing option 4 could mean missing an opportunity to provide for a more coherent and consistent legal regime of the Union for data processing and protection. Such a more coherent and consistent system could, on the long term, be based on a legal instrument providing for general rules in the area of data processing and protection. Such an instrument could have a guiding function and serve as orientation for further harmonisation of relevant legislation. Specific provisions in a legal instrument on the exchange of information under the principle of availability, on the contrary, are likely to contribute, to further fragmentation of the legal regime for data processing and protection under Title VI of the Treaty on European Union.

4.5. Option 5: Framework Decision on common standards for the processing and protection of personal data in the course of activities provided for by Title VI of the Treaty on European Union

The fifth option is a Framework Decision setting out common standards for the processing and protection of personal data in the course of activities provided for by Title VI of the Treaty on European Union. Contrary to Directive 95/46/EC and to the instruments adopted within the Council of Europe, a Framework Decision would provide for a complete system of legally binding provisions applicable to the direct exchange of information in the context of police and judicial cooperation in criminal matters while avoiding the weaker points of options 1 to 4.

A framework decision setting out general rules for data processing and data protection could not only confirm the fundamental principles already established for the Community and by the Council of Europe but also provide for a legally binding rules for all those questions that the various possible modalities of the exchange of information under the principle of availability have in common: not only principles relating to data quality but also more targeted rules for the criteria making data processing legitimate; obligations of the competent authorities when exchanging personal data; rights of the data subject, role of supervisory authorities, advisory body at EU level. It should also be borne in mind that this option would cover not only the principle of availability but more specific forms of police co-operation and exchange of information, such as the second generation of the SIS, the so-called "SIS II". However, a framework decision setting up common standards would not exclude the necessity of more specific rules where necessary.

It must be added, especially with regard to option 3, that the exchange of information under the principle of availability should not start until proper processing and protection personal data is ensured. Therefore, the two instruments on the exchange of information under the principle of availability and on data processing and protection should enter into force at the same time.

Furthermore, a separate instrument on data processing and protection could serve as a basis for further harmonisation and simplification of relevant legal instruments under Title VI of the Treaty on European Union.

4.6. Option 6: Legislative initiative involving all existing EU information systems or bodies (Europol, Eurojust)

The sixth and last option to be considered is a legislative initiative that aims at harmonising the rules for the processing and protection of personal data exchanged through *central information systems* and *bodies* (Europol, Eurojust) established at EU level as well as for the *direct exchange* between the Member States. This option is the most far reaching one. It avoids the weakness of options 1 to 5 while providing for a high level of harmonisation and simplification regarding data processing and protection under Title VI of the Treaty on European Union. In principle, this option is certainly the most preferable with regard to the consistency and coherence of the Union's policy on data processing and protection. However, as pointed out for option 5, more specific rules would have to be maintained or to be set up, where necessary. Secondly, the option would require a comprehensive legislative package containing not only a framework decision setting up general rules for the processing and protection of personal data that are exchanged directly between the Member States but also modifications of the exchange of information through existing EU information systems or bodies. Such initiative would go beyond what seems to be immediately necessary in view of the principle of availability. It would require much more consultations and might be confronted with objections from the bodies concerned. On the short term, it might be too ambitious and could even hamper the introduction of the principle of availability in January 2008.

5. IMPACTS OF THE POLICY OPTIONS

The possible positive or negative impact of measures on data processing and protection in the area of police and judicial cooperation have to be assessed, above all, with regard to the protection of fundamental rights directly protected by public security, such as the right to life and physical integrity; on the one hand and

fundamental rights, in particular the right to data protection, which may be affected by public security, on the other hand.

There is a close relation between the appropriateness of an option for achieving the objectives set out in Chapter 3 and possible impacts of an option. An option that is appropriate to achieve an objective regularly has a more positive impact on the area concerned, for example public security. On the other hand, it is difficult if not impossible to quantify the impact of the options described in chapter 4 on the basis of measurable criteria.

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

Positive or negative effects have to be assessed regarding fundamental rights affected by the protection of the fundamental rights directly safeguarded by public security, 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 can be stated if the data subject is generally well protected against violations of his/her fundamental rights, e.g. by unlawfully processing personal data. A negative impact has to be stated if the individual is likely to be forced to tolerate more restrictions than really necessary for the purpose of preventing and combating crime.

The consistency of the Union's policy on data processing and data protection could also be positively or negatively affected. This is important as consistency is likely to facilitate the application and implementation of the Union's legislation and, finally, to promote more efficiency in the area of police and judicial cooperation in criminal matters. At the same consistency is important taking into account the high level of data protection already guaranteed by Directive 95/46/EC. Therefore, the relation between the considered option on the one hand and already existing or developing legal instruments (Directive 95/46/EC, instruments under Title VI TEU) on the other hand has to be looked at.

Finally, possible positive or negative financial consequences have also to be taken into account. They might occur at the national level and/or for the Community budget. Given the value of the affected fundamental rights the factor "costs" seems to be of limited relevance.

5.1. Benefits and costs of Option 1: No legislative initiative

5.1.1. Respect for fundamental rights safeguarded by public security, in particular the right to life and physical integrity

As long as the exchange of information in the course of police and judicial cooperation at EU level is not substantially modified, a legislative initiative regarding data processing and protection seems to be unnecessary and is likely to have a rather neutral effect on public security. The decision not to launch a legislative initiative would not harm these fundamental rights. As soon as a comprehensive system of mutual rights and obligations for the exchange of information will be established under the principle of availability, the existing legal regime on data processing and protection is likely to be insufficient. Current

instruments are either too general or non binding or do not apply to the direct exchange of information between the Member States. The national legislation of at least some Member States do not exclude that information would not be transmitted to a police or judicial authority of another Member State for reasons of the level of data protection in the latter. Moreover, clear binding rules about the further processing of transmitted personal data do not exist.

5.1.2. Respect of fundamental rights affected by public security, in particular the right to data protection

Currently, data processing and protection with regard to the direct exchange of information between the Member States in the context of preventing and combating crime is subject to national law, which, of course, has to be in line with the Data Protection Convention of the Council of Europe. In general, Member States respect fundamental rights, in particular the right to data protection. Without any further changes at EU level of the exchange of information in the area of police and judicial cooperation the absence of legislative initiative would neither improve nor weaken the level of data protection in the Member States. The impact on fundamental rights would be rather neutral.

5.1.3. Consistency of the Union's data protection policy

The option of submitting no legislative proposal does not result in modifications of the Union's existing legal regime for data processing and protection. On the other hand, one could argue that the present situation is already characterised by the inconsistency of data protection rules for police and judicial cooperation in criminal matters. The European Parliament, in particular, has already expressed its dissatisfaction with the present situation. Insofar the option of doing nothing would rather maintain current inconsistency than provide for an approach to overcome it. Insofar the impact of option is rather negative.

5.1.4. Costs

Option 1 is unlikely to generate any costs.

5.2. Benefits and costs of Option 2: Application of Directive 95/46/EC

5.2.1. Respect for fundamental rights safeguarded by public security, in particular the right to life and physical integrity

Directive 95/46/EC does not cover activities aimed at preventing or combating crime. The specific situation of police, judicial and other competent authorities has not been addressed but excluded from the scope. Insofar applying the Directive would largely mean basing its national implementation exclusively on Article 13 which provides for exceptions from a number of principles laid down in the Directive. At the end the impact of rules on data processing and protection would largely depend on the discretion of the Member States. So far this did not cause any harm for public security. In view of the implementation of the principle of availability, however, the Directive would be insufficient and could, without modifications, even hamper this implementation.

5.2.2. Respect of fundamental rights affected by public security, in particular the right to data protection

In general, the Directive provides for a high level of data protection. In principle, its application to police and judicial cooperation in criminal matters is likely to transpose this level to that area. On the other hand, the use of exceptions provided for

in Article 13 of the Directive gives Member States huge discretion. With regard to preventing and combating crime the provisions of the Directive are not precise enough. Although the high level of data protection provided for in the first pillar has to be acknowledged, it is not sure if the same EU wide level would be established for the third pillar.

5.2.3. Consistency of the Union's data protection policy

Applying the Directive is likely to promote a higher degree of consistency of the Union's data protection policy as only one instrument would, in general, apply in the first and in the third pillar.

5.2.4. Costs

Applying the Directive is unlikely to result in additional costs. In general, Member States would have neither to adapt their legislation nor to introduce new bodies or systems. Already existing bodies established by the Directive (in particular Article 29 Working Party) including secretarial services would also be used for the discussion of third pillar issues. Due to increasing number of issues to be discussed this might result in some (maybe two or three) more meetings per year.

5.3. Benefits and costs of Option 3: Legislative initiative once the modalities for the exchange of information under the principle of availability have been defined

5.3.1. Respect for fundamental rights safeguarded by public security, in particular the right to life and physical integrity

This option might promote the exchange of information under the principle of availability even without appropriate data protection provisions being in force. This is likely to have a positive impact on the fundamental rights safeguarded by public security. On the other hand, the Hague Programme stresses that such a situation should be avoided.

5.3.2. Respect of fundamental rights affected by public security, in particular the right to data protection

Rather negative impact. From a data protection point of view the exchange of information under the principle of availability should not start until appropriate data protection provisions are in force.

5.3.3. Consistency of the Union's data protection policy

The considerations made for option 1 can be referred too as option 3 would mean, at least temporarily: no legislative initiative as far as data protection is concerned. Contrary to option 1 option 3 could even worsen the inconsistency of the data protection regime in the third pillar as the latter might be confronted with new modalities of the exchange of information without having sufficiently addressed data protection issues.

5.3.4. Costs

Additional costs are unlikely to occur.

5.4. Benefits and costs of Option 4: Specific provisions in a legal instrument on the exchange of information under the principle of availability

5.4.1. Public security and

5.4.2. Respect of fundamental rights, in particular the right to data protection

Option 4 could provide for targeted rules on data processing and data protection for the exchange of information for the purpose of preventing and combating crime in view of the introduction and implementation of the principle of availability. It could ensure an appropriate data protection regime and avoid the disadvantages of options 1, 2 and 3. Therefore, the impact on fundamental rights and public security is likely to be positive. Particularly, concerning data protection, these adequate and targeted rules of option 4 would ensure that the data subject is generally well protected against unlawful processing of personal data.

5.4.3. Consistency of the Union's data protection policy

The impact on the consistency of the Union's data protection policy might be less positive. A set of data protection provisions in an instrument on the principle of availability in addition to existing instruments containing data protection provisions is likely to increase the complicatedness and thus the inconsistency of the data protection regime for police and judicial cooperation in criminal matters. Insofar the impact is rather negative.

5.4.4. Costs

Option 4 is unlikely to result in considerable additional costs. In general, Member States are likely to adapt their legislation. New bodies or systems are most probably not necessary. An advisory body for data protection issues related to the principle of availability (comparable to the Article 29 Working Party) including secretarial services would cause costs for a number of meetings per year.

5.5. Benefits and costs of Option 5: Framework Decision on common standards for the processing and protection in the course of activities provided for by Title VI of the Treaty on European Union

5.5.1. Respect for fundamental rights safeguarded by public security, in particular the right to life and physical integrity

Option 5 could 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 by Title VI of the Treaty on European Union. It can ensure an appropriate data protection regime and avoid the disadvantages of options 1, 2 and 3. The impact on the fundamental rights protected by public security (life and physical integrity) can be expected to be positive.

5.5.2. Respect of fundamental rights affected by public security, in particular the right to data protection

For the reasons set out under 5.5.1 a positive impact can also be expected on the respect of fundamental rights. As it is the case under 5.4.2, the adequate and targeted rules of the data protection regime would ensure that the data subject is generally well protected against unlawful processing of personal data.

5.5.3. Consistency of the Union's data protection policy

Contrary to option 4 a comprehensive framework decision can be expected to have a more positive impact on the consistency of the Union's policy on data protection. Option 5 would not only cover the exchange of information under the principle of availability but also more specific forms of police co-operation and exchange of information, such as the second generation of the SIS, the so-called "SIS II". It could therefore be considered at least as a first step towards a less difficult and more transparent legal regime on data protection under Title VI TEU. Moreover, a framework decision could follow as far as possible the example of Directive 95/46/EC and contribute to a more consistent data protection policy ensuring a high level of data protection in *both* the first and the third pillar.

5.5.4. Costs

Option 5 is unlikely to result in considerable additional costs. In general, Member States are likely to adapt their legislation. New bodies or systems are most probably not necessary. An advisory body for data protection issues related to police and judicial cooperation in criminal matters (comparable to the Article 29 Working Party) including secretarial services would cause costs for a number of meetings per year.

5.6. Benefits and costs of Option 6: Legislative initiative involving all existing EU information systems or bodies

5.6.1. Respect for fundamental rights safeguarded by public security, in particular the right to life and physical integrity

Option 6 could provide for targeted rules on data processing and data protection for the exchange of information for the purpose of preventing and combating crime not only in view of the principle of availability but for all kinds of exchanging information in the course of activities provided for by Title VI TEU. It could avoid the disadvantages of options 1, 2 and 3 and result in an even more comprehensive data protection regime than possible on the basis of option 5. In general, the impact on the fundamental rights safeguarded by public security is likely to be positive. However, the introduction of such a comprehensive legal regime could be confronted with considerable objections referring to proven instruments (for example for Europol and Eurojust) that comply with specific functions. At the end such controversies might slow down the adoption of those provisions, which are really necessary in view of the principle of availability. Insofar option 6 could even be contra productive and have a negative impact on public security.

5.6.2. Respect of fundamental rights affected by public security, in particular the right to data protection

A comprehensive and transparent legal framework can be expected to have a positive impact on fundamental rights. Particularly, concerning data protection, these comprehensive and targeted rules would ensure that the data subject is generally well protected against unlawful processing of personal data.

5.6.3. Consistency of the Union's data protection policy

Option 6 is likely to result in an even higher degree of consistency of the Union's data protection policy than possible on the basis of option 5. The impact can be expected to be very positive. However, taking into account the considerations explained under 5.6.1 the way to the adoption of the comprehensive system

envisaged by option 6 could be rather long. A two-step-approach as still possible under option 5 could, on the long term, end with the same result.

5.6.4. Costs

No differences to option 5.

5.7. Impact summary table

The following table will summarise the probable impact of the different policy options in view of the introduction of the principle of availability:

Policy options	Advantages	Drawbacks
No legal initiative	No additional costs	Negative impact on fundamental rights and public security; no added value for consistency of the Union's data protection policy
Application of Directive 95/46/EC	High level of data protection, positive impact on respect of fundamental rights, low additional costs	Not precise enough for the area of preventing and combating crime, probably negative impact on fundamental rights directly protected by public security in view of the implementation of the principle of availability
Legislative initiative once the modalities for the exchange of information under the principle of availability have been defined	In principle positive impact on fundamental rights directly protected by public security, no additional costs	Not fully in line with data protection requirements of The Hague Programme, negative impact on respect of fundamental rights affected by public security and on consistency of the Union's data
Specific provisions in a legal instrument on the exchange of information under the principle of availability	Positive impact on respect of fundamental rights and public security, low additional costs	Negative impact on consistency of the Union's data protection policy
Framework Decision on common standards for the processing and protection of personal data in the course of activities provided for by Title VI of the Treaty on European Union	Positive impact on fundamental rights and public security, and consistency of the Union's data protection policy, low additional costs	Lower degree of harmonisation directly envisaged than in option 6
Legislative initiative involving all existing EU information systems or bodies (Europol, Eurojust)	Positive impact on fundamental rights and public security, very positive impact on consistency of the Union's data protection policy	Very ambitious, possibly confronted with considerable objections, possibly not feasible within the time schedule for the implementation of the principle of availability

6. COMPARING THE OPTIONS

Option 1 (no legislative initiative) has to be excluded as it has no real positive impact on or no added value for the areas concerned. The high level of data protection makes option 2 very attractive (Application of Directive 95/46/EC). However, it is not adapted to the third pillar, leaving too much lea-way to interpretation. Given drawbacks of the option it should be considered if the same level of protection could be ensured by one of the other options. Option 3 (legislative initiative once the modalities for the exchange of information under the principle of availability have been defined) should be excluded because of its drawbacks regarding data protection. Options 4 (Specific provisions in a legal instrument on the exchange of information under the principle of availability), 5 (Framework Decision on common standards for the processing and protection of personal data in the course of activities provided for by Title VI of the Treaty on European Union) and 6 (Legislative initiative involving all existing EU information systems or bodies (Europol, Eurojust)), on the contrary, could be further developed in a way that safeguards the advantage of option 2. Looking more closely at options 4, 5 and 6, their main difference is the impact on the consistency of the Union's data protection policy. The latter is only promoted by options 5 and 6. On the long term, option 6 is more attractive and aims at a higher degree of harmonisation. The implementation of option 6, however, might take more time than foreseen for the implementation of the principle of availability. Furthermore, it has to be taken into account that largely satisfying rules on data processing and protection do exist for the exchange of information through Europol and Eurojust. Further harmonisation including all information systems and bodies established at EU level is useful but seems to be less urgent than a quick introduction of the principle of availability. The latter can be accompanied by an instrument on data processing and protection, which could then serve as the basis for further harmonisation. Such a two step approach would address the short term necessities as well as, on the long term, further harmonisation of the legislation on data processing and data protection under Title VI TEU. Therefore, the Commission recommends option 5 (Framework Decision on common standards for the processing and protection of personal data in the course of activities provided for by Title VI of the Treaty on European Union).

7. MONITORING AND EVALUATION

The proposed option, i.e. a Framework Decision on common standards for the processing and protection of personal data in the course of activities provided for by Title VI of the Treaty on European Union, shall be evaluated in accordance with the usual procedures under this Title VI. 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 assess before December 2007 the extent to which Member States have taken the measures necessary to comply with this Framework Decision.

Furthermore, a working party shall be established according to the Framework Decision. The Working Party shall be composed of a representative of the supervisory authority or authorities designated by each Member State and of a representative of the authority or authorities established for the Community

institutions and bodies, and of a representative of the Commission. The European Data Protection Supervisor and the chairpersons of the joint supervisory bodies set up under Title VI of the Treaty on European Union shall be entitled to participate or to be represented in meetings of the Working Party.

The Working Party shall

- examine any question covering the application of the national measures adopted under this Framework Decision in order to contribute to the uniform application of such measures,
- give an opinion on the level of protection in the Member States and in third countries, in particular in order to guarantee that personal data are transferred in compliance with the Framework Decision to third countries or international bodies that ensure an adequate level of data protection,
- advise the Commission and the Member States on any proposed amendment of this Framework Decision, on any additional or specific measures to safeguard the rights and freedoms of natural persons with regard to the processing of personal data for the purpose of the prevention, investigation, detection and prosecution of criminal offences and any other proposed measures affecting such rights and freedoms.

Therefore, the working party will play a substantial role for the continuous monitoring and evaluation and, if necessary, the review or further development of the Framework Decision. In this context the working party will have to take into account indicators such as the number of complaints of the data protection authorities as well as of appeals of data subjects in the Member States relating to non-compliance with this Framework Decision.