Spring Conference of European Data Protection Authorities, Cyprus 10-11 May 2007

DECLARATION

The European Union initiated several initiatives to improve the effectiveness of law enforcement and combating terrorism in the European Union. In this context, the exchange of law enforcement information in accordance with the principle of availability is a key issue in the third pillar cooperation.

Monitoring these developments, the Conference of European Data Protection Authorities already called on the Members of the European Union and the Commission, the Council and the European Parliament to establish strong and harmonized data protection safeguards[1].

The various forms in which this concept of "availability" is used, explicitly or implicitly, in developing strategies and legal instruments to improve effectiveness in law enforcement, makes it also necessary to establish a comprehensive framework for assessing the use of this concept. By creating such a framework, guidance will be provided to assess every proposal that uses the existence of personal data as a chance to improve the effectiveness of law enforcement. Such a framework may thus contribute to a balanced assessment of the interrelation between public security and the fundamental right of protection of personal data.

The Conference has adopted the attached Common Position on the use of the availability principle in law enforcement. This Common Position includes a checklist for assessing any proposal using availability of personal data as its basis.

This paper and checklist are addressed specifically to all EU institutions as well as national parliaments as a constructive contribution to respect and strengthen the civil liberties of the citizens living in the EU when expanding the possibilities for the use of information by law enforcement authorities.

---

[1] Krakow Declaration, 25-26 April 2005,
Budapest Declaration, 24-25 April 2006.

Common position of the European Data Protection Authorities on the use of the concept of availability in law enforcement

Adopted on 11 May 2007

Executive summary

In the context of combating terrorism and improving internal security, the European Union initiated several initiatives to improve the effectiveness of law enforcement in the European Union, using the concept of availability as guiding principle for the exchange of law enforcement in third pillar cooperation.

The various forms in which this concept of availability is used, explicitly or implicitly, in developing strategies and legal instruments to improve effectiveness in law enforcement, makes it necessary to establish a comprehensive framework for assessing the data protection aspects relating to the use of this concept. By creating such a framework, guidance will be provided to asses every proposal that uses the existence of personal data as a chance to improve the effectiveness of law enforcement. Such a framework may thus contribute to a balanced assessment of the interrelation between public security and the fundamental right to the protection of personal data as enshrined in the Charter of Fundamental Rights of the European Union.

The European Data Protection Authorities, stressing the need to create such a framework, have developed some conditions and guidelines for assessing the use of the availability concept in the following Common Position paper and checklist. This checklist can be used for assessing every proposal that uses the availability of personal data as stepping stone to improve law enforcement. The European Data Protection Authorities urge the Commission, Council and European Parliament to use this checklist when developing, assessing and adopting any proposal using availability of personal data as a stepping stone to improve law enforcement or the cooperation between law enforcement authorities.

Common position on the use of the concept of availability in law enforcement

1. Introduction

In the context of combating terrorism and improving internal security, the European Union initiated several initiatives to improve the effectiveness of law enforcement in the European Union.
Article 29 TEU aims at providing citizens with a high level of safety within an area of freedom, security and justice. This area of freedom, security and justice is gradually developing and leads to the abolishment of the borders between the Member States for law enforcement information. However, the enforcement powers of the Member States are still bound by these national borders.

Within this context, the exchange of law enforcement information using the concept of availability has become a key issue in third pillar cooperation:
- as an important instrument in realising a free flow of law enforcement information, not hampered by internal borders,
- by providing for safety for the citizen by means of facilitating the combat of trans-border crime,
- by respecting the protection of fundamental rights and freedoms of the citizen, in particular the rights to privacy and data protection.

These three objectives must be met in a balanced way. This is not obvious in view of the specific character of law enforcement and also in the light of the trend in police work to increasingly use personal data for proactive research. A guiding principle in law enforcement seems to be: when data are needed, they should be used. Or, even clearer: when data are available they can be used.

This subject clearly demonstrates the close interrelation between public security and the fundamental right to the protection of personal data as enshrined in the Charter of Fundamental Rights of the European Union.

An important element in that interrelation is mutual trust. Mutual trust (and mutual recognition) is an essential condition for exchange of law enforcement information. Governments and government authorities are only prepared to effectively share information with (authorities in) other Member States if it is assured that these other Member States use this information with respect of appropriate legal conditions, for reasons of data protection and security.

Already adopted EU legislation as well as recent initiatives are not limited to stimulating the exchange of personal data between law enforcement authorities of personal that is data already processed by those authorities. Some also focus on the use for law enforcement purposes of personal data that are processed by parties in the private and public sector or in European data bases. When there seems to be an indication that these might be needed for law enforcement purposes, these data are (proposed to be) made available to law enforcement authorities.

The various forms in which this concept of availability is used, explicitly or implicitly, in developing strategies and legal instruments to improve effectiveness in law enforcement, makes it necessary to establish a comprehensive framework for assessing the data protection aspects relating to the use of this concept. By creating such a framework, guidance will be provided to assess every proposal that uses the existence of personal data as a chance to improve the effectiveness of law enforcement.

The European Data Protection Authorities, stressing the need to create such a framework, have developed some conditions and guidelines for assessing the use of the availability concept. The European Data Protection Authorities urge the Commission, Council and European Parliament to use these when developing, assessing and adopting any proposal using availability of personal data as a stepping stone to improve law enforcement or the cooperation between law enforcement authorities.

2. Scope of the availability concept

The strategy of the European Union as defined in The Hague Programme on strengthening freedom, security and justice [2] aims that with effect from 1 January 2008, the exchange of law enforcement information should be governed by the principle of availability.

Following that strategy the Commission presented on 12 October 2005 its proposal for a Council Framework Decision on the exchange of information under the principle of availability[3]. This proposal lays down an obligation for the Member States to give access to or to provide certain types of information available to their authorities (see Recital 6).

The principle of availability as used in The Hague Programme and the proposed Framework Decision mean that, throughout the European Union, a law enforcement officer in one Member State who needs information in order to perform his duties should be able to obtain this from another Member State and that the law enforcement authority in the other Member State which holds this information will make it available for the stated purpose. The proposed Framework Decision limits the principle of availability by stating that the decision does not entail any obligation to collect and store information for the sole purpose of making it available (Article 2(1)).

Sharing available information such as personal data, is already foreseen in existing EU legislation and multilateral conventions. Recent proposals for improving the cooperation between law enforcement authorities also use the availability concept as guiding principle. However, in all these legal instruments and proposals, availability of personal data is presented in different forms and modalities leading to different consequences. These differences make it necessary to further explore the scope of this concept.

---

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

[3] COM (2005) 490.

One of the first examples of sharing personal data as a specific aspect of effective cooperation between European law enforcement authorities is perhaps the Convention of 19 June 1990 implementing the Schengen Agreement of 14 June 1985[4]. Processing personal data of specific categories of persons and making those available - by using one central information system - for different authorities in the States that implemented the Schengen Convention is seen as a necessary compensatory measure for creating a high level of security in an area of free movement of persons.

Another step in improving cooperation between law enforcement authorities was marked by the Europol Convention[5] and Eurojust Decision[6]. Two European offices were established with, among other tasks, a specific task to facilitate the exchange of law enforcement information.

These forms of cooperation may be characterised as cooperation by expressing the intention to share information without a specific obligation to do so.

More recent examples of making personal data available for law enforcement authorities are the Framework Decision on simplifying the exchange of information and intelligence between law enforcement authorities of the Member States of the European Union[7] and the Treaty of Prüm of 27 May 2005. These two legal instruments introduce a new element in law enforcement cooperation: Member States are in principle obliged to make personal data available. The use of wordings as: "*shall provide at the request*" (Framework Decision) and "*will allow access… and right to consult*" (e.g. Article 3(1) Prüm Treaty) clearly indicate the obliging character of making data available.

---

[4] OJ L 239, 22.9.2000, p.19.

[5] OJ C 316, 27.11.95, p.1.

[6] OJ L 63, 6.3.2002, p.1.

[7] OJ L 386, 29.12.2006, p.89.

The Prüm Treaty furthermore introduces an obligation to set up certain data files to facilitate the prevention and prosecution of crimes. Contracting Parties must for example guarantee the availability of reference indexes of fingerprints (Article 8).

The existing more or less voluntary exchange of information is in these areas not only replaced by an obligation to provide information, but also by an obligation to create for certain categories of personal data an infrastructure enabling other law enforcement authorities to have access to available data.

Such an obligation to make information available is not necessarily limited to law enforcement authorities. For example, Recital 19 of Directive 2006/24/EV on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC, specifically mentions that "*it is necessary to ensure that retained data are made available*". It is ensured on a European level that certain categories of data processed by private parties should be made available for law enforcement.

The concept of availability is also an important subject of the Communication from the Commission to the Council and the European Parliament of 24 November 2005 on improved effectiveness, enhanced interoperability and synergies among European databases in the area of Justice and Home Affairs[8]. Sharing available information by linking databases is a key item in future thinking in the European Union.

Other initiatives such as the new legal basis of the second generation Schengen Information System and the creation of the Visa Information System also contain aspects of the availability concept. Personal data processed for a specific purpose is made available for other purposes such as law enforcement.

In view of this variety of manifestations of the concept of availability as key factor for the improvement of effectiveness of law enforcement and their impact on the fundamental right

[8] COM(2005) 597.

of protection of personal data, the European Data Protection Authorities stress the need to contextualize the practice of the use of the availability concept in a comprehensive way. Any action of harmonising the processing of personal data, either by introducing obligations to retain personal data or by introducing an obligation to set up specific data files, and the introduction of an intention or obligation to make these personal data available for law enforcement authorities or for European or international institutions involved with law enforcement, should be seen as implementation of the concept of availability.

Using this scope, the European Data Protection Authorities have explored its implications in perspective of the applicable data protection legislation.

3. Applicable law

In addition to the right to respect for private and family life guaranteed by Article 8 of the ECHR and reaffirmed by Article 7 of the Charter of Fundamental Rights of the European Union, the new fundamental right to data protection is enshrined in Article 8 of the Charter.

The ECHR allows interference with the right to privacy if necessary for the interests referred to in the second paragraph of Article 8 and when justified by those interests; such interference must take account of the principle of proportionality. Article 8 of the Charter of Fundamental Rights expands on this, stipulating that personal data must be processed fairly for specified purposes, and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. This legitimate basis has also to fulfill the conditions of proportionality.

The 1981 Council of Europe Convention for the Protection of Individuals to Automatic Processing of Personal Data (Convention 108) provides more specific principles for data protection also applicable in the Third Pillar. There is also a Recommendation (No. R(87) 15) with specific data protection provisions for the use of personal data in the police sector,

which was adopted in 1987 by the Committee of Ministers to Member States regulating the use of personal data in the police sector.[9]

The Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data[10] provides for a harmonized data protection regime in the European Union. Although activities referred to in Titles V and VI of the Treaty on European Union fall outside the scope of this directive, Member States apply the general data protection principles to law enforcement activities.

The Regulation 45/2001 of the European Parliament and of the Council of 18 September 2000[11] provides rules on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data. The principles of this Regulation are used by defining the data protection regime applicable to the processing of personal data in European data bases such as the Visa Information System and the second generation Schengen Information System.

The Europol Convention and Eurojust Decision contain specific data protection regime for these organizations based on the general data protection principles as defined in the Convention 108 and the Recommendation No. R(87) 15 referred to above.

Concerning data processing by private parties, public parties and the European Institutions and in European data files, the applicable EU laws contain a fundamental principle on the lawfulness of the processing of personal data: data should be collected for explicit and legitimate purposes and not further processed in a way incompatible with those purposes. An exemption or restriction is only allowed when provided for by law and when this constitutes a necessary measure to safeguard national and public security or the prevention, investigation, detection and prosecution of criminal offences. The definition used in those

---

[9] Recommendation No. R (87) 15, of 17 September 1987

[10] OJ L 281, 23.11.1995, p. 31.

[11] OJ L 8, 12.1.2001, p.1.

legal instruments for processing of data includes the disclosure by transmission, dissemination or otherwise making available.

In those situations where applying the availability concept, data which are originally processed for purposes outside the law enforcement scope are used for law enforcement, the exemption to the fundamental rule of purpose limitation needs to fulfill all the conditions for the use of this exemption.

4. Implementing the availability concept

The success of effective law enforcement will be dependant on the information position of law enforcement authorities, the possibility to collect within the limits of the law information, the quality and use of these data and the capability to share these data with other law enforcement authorities. The different forms of law enforcement cooperation in the European Union as described in Chapter 2, cover all these aspects.

In respect of all the initiatives to exchange personal data between law enforcement authorities in the European Union and the exchange with third States and parties, the European Data Protection Authorities already declared 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."*[12]

In that respect, the European Data Protection Authorities welcome the draft Council Framework Decision on the protection of personal data processed in the framework of police- and judicial cooperation in criminal matters[13]. A harmonised and high level of data protection in the area of law enforcement as should be ensured by a Council Framework

[12] Krakow Declaration, 25-26 April 2005.

[13] COM (2005) 475.

Decision is now considered a conditio sine qua non for law enforcement in the European Union.

However, it should be stressed that such a harmonised data protection framework does in itself not present a comprehensive tool for assessing the implementation of the availability concept in all varieties as described in Chapter 2. That framework only applies when personal data are already processed by law enforcement authorities. Furthermore, the discussions on that draft Framework Decision are still taking place in the Council.

Since the variety in the use of the availability concept results in the application of different legal instruments, a comprehensive framework for assessing the use of this concept should therefore cover all aspects of the use of the availability concept. Such a framework should be a separate instrument also to be used supplementary to existing legislation.

5. A comprehensive framework for assessing the use of the availability concept.

Law enforcement is dependant on information. In principle two sources of information are used: information already processed by law enforcement authorities and information that is processed by others. This distinction is somewhat artificial since data processed by law enforcement authorities may have been obtained from private or public authorities.

When personal data are processed by private or public authorities, the data protection principles as defined in Directive 95/46/EC will be guiding. When these data are processed either by European institutions or in European data files, the principles of Regulation 45/2001 and/or the applicable specific rules for these files will apply.

As already stated, the use of these data for law enforcement purposes will in general constitute an exemption to the fundamental rule of purpose limitation and is only allowed when provided for by law and when this constitutes a necessary measure to safeguard national and public security or the prevention, investigation, detection and prosecution of criminal offences.

In case data are already processed by law enforcement authorities the (draft) Council Framework Decision on the protection of personal data processed in the framework of police and judicial co-operation in criminal matters will provide for a necessary legal data protection framework for the processing and exchange of information between law enforcement authorities. However, new initiatives for processing these data may be introduced, based on the concept of availability.

In assessing whether an exemption is needed and in compliance with the formal conditions or when assessing new initiatives for making law enforcement data available, it will be necessary to focus on the different conditions provided for by the applicable data protection rules.

The first condition relates to the obligation that any measure should be provided for by law.
This law must comply with strict criteria such as being clear, simple and precise: they are to be transparent and readily understandable for everybody. According to the case-law of the Court of Justice, the principle of legal certainty requires that legislation must be clear and precise and its application foreseeable by individuals. Furthermore, legislation must always determine the grounds, purpose and the conditions for the processing, as well as install an adequate and effective system of independent supervision.

The second condition which needs to be complied with is that any measure should be necessary and proportionate. It is especially the assessment of this aspect that needs a comprehensive approach. Such an approach should include the following assessment steps:

A. Evaluation of already existing legal measures allowing the processing including the exchange of data.

Are these measures not sufficient or is their implementation and follow up not effective? When a legal measure is effectively used but does apparently not provide for a sufficient and effective element in the fight against crime, this might be an

indication that another measure is needed. However, when the evaluation demonstrates that already existing possibilities are not used sufficiently, this may create considerable doubt whether a proposed new measure will be a justified.

In case this assessment indicates that the legal measure could be justified, the following conditions should be met:

B. Proportionality

Effective enforcement, but with a minimum interference with privacy. This means a proportionality-test with the following elements:

* The measure must be appropriate, which means its contribution to law enforcement must be clearly demonstrated.

* A measure with less impact can not lead to the same result.

* A balance must exist: where an impact on data protection may be justified in order to fight terrorism and other serious crime (as referred to in Article 2(2) of the Framework Decision on the European Arrest Warrant), this does not mean that these data may be made available to fight minor misdemeanours.

* The legal instrument should be subject of compulsory evaluation.

The third condition relates to the categories of data to be processed and other specific conditions.

Different types of data are involved: ranging from identification data (used for both identification of data subject and for contacting him) and general and specific descriptive data (e.g. intelligence) to types identified on the basis of their biometrics (e.g. fingerprint and DNA digital representation) and sensitive data (as referred to in Article 8 of Directive 95/46). Similarly, different types of data subjects are involved: suspects, non suspects, witnesses, convicted or acquitted persons. The following points should be taken into account:

A. Legislation must distinguish between these data and must provide for complementary safeguards in respect of processing data that are likely to present specific risks to the rights and freedoms of the data subject, in particular sensitive data

by introducing a sliding scale of protective measures, in which the characteristics of the data determine special conditions and limitations for their use. It should include criteria for a clear distinction between personal data, differentiating categories of personal data and their availability for specific categories of crime. For example, persons acquitted from a charge or against whom no charges are pressed should clearly be distinguished from convicted persons. Data on non-suspects and witnesses should be clearly distinguished from data on suspects.

Such a distinction could be linked with the distinction between different categories of persons in Article 4(3) of the Commission proposal for a draft Council Framework Decision on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters.

B. Specific measures to assess the quality of data must be introduced to guarantee the highest possible level of data quality before data are to be made available. In view of the impact of the use of data for law enforcement purposes sufficient technical and organisational measures and procedures must be in place to guarantee the quality of data. In case such guarantees can not be provided for, this must be indicated and the use of those data must be limited to a specific law enforcement activity with additional safeguards. An obligation to inform the recipient of personal data of any change in those data must be compulsory.

C. The use of biometric data in law enforcement requires extra safeguards for their use. Especially the use of these data for identification purposes, sometimes using systems that process huge amounts of these data such as the new Schengen information System must be accompanied by procedures for the individual to have the result of the comparison rechecked.

D. Specific processing operations that are likely to present specific risks (e.g. fishing expeditions, data mining, specific surveillance techniques) require extra safeguards for the use of these data and the monitoring of the use of these operations.

E. It will be important to ensure with technical and organisational measures and procedures that the receivers of personal data are supplied with the necessary information to use the data for the purposes for which they were exchanged and to keep them up to date.

F. When an initiative or proposal makes a choice between processing of personal data on a central level or decentralised, this choice may not only be motivated by reasons of operability. Such a choice must also take into account the need to guarantee the highest possible level of data quality and data protection standards. When decentralised processing provides for the best safeguards, central processing should not be an option.

The fourth condition relates to the access to these data.

Routine access to personal data must be prohibited. Access should be limited to specific cases or a specific law enforcement task, and control of the use of this access must be sufficiently safeguarded. Recipient authorities must be clearly identified**.** When direct access to data is proposed, the use of index or hit-no-hit systems and sufficient access controls are required.

The fifth condition relates to control and supervision.

In addition to the standard competences of law enforcement authorities, judicial authorities and data protection authorities for controlling and supervising data processing activities that are likely to present specific risks to the rights and freedoms of the data subject should be accompanied by additional and tailor made measures of control and supervision of all operational activities including the use and mis-use of personal data.
Specific provisions are needed preventing difficulties arising from the exchange of data between Member States. Since those data are available within several jurisdictions, it must be ensured that control and supervision have effect in all jurisdictions involved.

6. Conclusion

The European Data Protection Authorities recognize that information and personal data are essential for effective law enforcement. They would reiterate, however, that any measure in which the concept of availability is used ought to be proportionate, respecting the fundamental rights of the individual. This Common Position and the checklist are addressed specifically to the EU institutions as a constructive contribution to current initiatives. It presents the conditions that must be met to maintain a high level of data protection in the field of law enforcement. The European Data Protection Authorities are, of course, willing to contribute further to ensuring that the process of improving law enforcement is combined with respect to fundamental rights.

Checklist assessing any measure implementing the availability concept in law enforcement.

I. Law and evaluation

Any measure must be provided for by law.

This law must comply with strict criteria such as being precise and creating certainty and foreseeability.

Furthermore, legislation must always:

* Determine the grounds,
* Purpose and
* The conditions for the processing.
* Install an adequate and effective system of independent supervision.

II. Necessity and proportionality

The measure should constitute a necessary safeguard.

A. Evaluation of already existing legal measures allowing the processing including the exchange of data.

* Are these measures not sufficient?
    - When a legal measure is effectively used but does apparently not provide for a sufficient and effective element in the fight against crime, this might be an indication that another measure is needed.
* Is their implementation and follow up not effective?
    - When the evaluation demonstrates that already existing possibilities are not used sufficiently, this may create considerable doubt whether a proposed new measure will be a justified exemption to the rule of purpose limitation.
* In case this assessment indicates that the legal measure could be justified, the following conditions of proportionality should be met:

B. Proportionality

* The measure should be designed to achieve

III. *Specific conditions*

Different types of data are involved: ranging from identification data (used for both identification of data subject and for contacting him) and general and specific descriptive data (e.g. intelligence) to types identified on the basis of biometrics (e.g. fingerprint and DNA digital representation) and sensitive data (as referred to in Article 8 of Directive 95/46). Similarly, different types of data subjects are involved: suspects, non suspects, witnesses, convicted or acquitted persons**.** The following points should be taken into account:

A. Legislation must:

* Distinguish between these data,
* Provide for specific and complementary safeguards in respect of processing data that are likely to present specific risks to the rights and freedoms of the data subject, in particular the use of sensitive data by introducing a sliding scale of protective measures, in which the characteristics of the data determine special conditions and limitations for their use.
* Include criteria for a clear distinction between personal data, differentiating categories of personal data and their availability for specific categories of crime. (For example, persons acquitted from a charge or against whom no charges are pressed should, for example clearly be distinguished from convicted persons. Data on non-suspects and witnesses should be clearly distinguished from data on suspects.)

B. Specific measures to assess the quality of data must be introduced to guarantee the highest possible level of data quality before data are to be made available. In view of the impact of the use of data for law enforcement purposes sufficient technical and organisational measures and procedures must be in place to guarantee the quality of data. In case such guarantees cannot be provided for, this must be indicated and the use of those data must be limited to a specific law enforcement activity with additional safeguards. An obligation to inform the recipient of personal data of any change in those data must be compulsory.

C. The use of biometric data in law enforcement requires extra safeguards.

F. When an initiative or proposal makes a choice between processing of personal data on a central level or decentralised, this choice must not only be motivated by reasons of operability. Such a choice must also take into account the need to guarantee the highest possible level of data quality and data protection standards. When decentralised processing provides for better safeguards, central processing should not be an option

IV. Access by law enforcement authorities to personal data

* Routine access to personal data must be prohibited.
* Access must be limited to specific cases or a specific law enforcement task.
* Control of the use of this access must be sufficiently safeguarded.
* When direct access to data is proposed, the use of index or hit-no-hit systems and sufficient access controls are required.
* The recipient authorities must be clearly identified.

V. Control and supervision

***** In addition to the standard competences of law enforcement authorities, judicial authorities and data protection authorities for controlling and supervising data processing, activities that are likely to present specific risks to the rights and freedoms of the data subject should be accompanied by additional and tailor made measures of control and supervision of all operational activities including the use and mis-use of personal data**.**