

OPINION

Introduction

The 2005 Spring Conference of European Data Protection Authorities has adopted the following opinion on:

The draft Framework Decision on simplifying the exchange of information and intelligence between law enforcement authorities of the Member States of the European Union, in particular as regards serious offences including terrorist acts. 4 June 2004 (10215/04)

Background

Citing the European Council's declaration on combating terrorism of 25 March 2004, which called on the Council to improve and simplify the exchange of information between the law enforcement authorities of Member States, the Kingdom of Sweden has prepared a draft Framework Decision with the objective of creating 'a common and simplified framework for the exchange of information and intelligence between competent law enforcement authorities of the Member States'.¹

The Framework Decision

The explanatory memorandum claims that existing differences in national legislation and administrative structures in the Member States are the main obstacles to the exchange of information and intelligence within the EU, and that a Framework Decision is the best way of addressing these problems. There follows a brief summary of the relevant provisions of the draft Framework Decision.

¹ Taken from page 4 of the Explanatory Memorandum

The proposed Framework Decision would require law enforcement authorities in Member States to supply certain information and intelligence to law enforcement authorities in other Member States on request. Specifically, the Decision seeks to 'establish the rules under which Member States' law enforcement authorities . . . can exchange existing information and intelligence for the purpose of conducting crime investigations or crime intelligence operations' (Article 1 (1)).

Such information would have to be provided without delay and preferably within the timeframe requested (Article 4 (3)), and law enforcement authorities should only decline a request for information if able to rely on one of the exemptions available under the Decision (Article 11).

All offences punishable by a maximum sentence of 12 months or more would be covered by the Decision (Article 3). The draft Decision also includes a list of offences that are deemed more serious, and which therefore require information to be made available no more than 12 hours after a request (Article 4 (a) (2)).

Data may be exchanged on: those suspected of committing an offence covered by Article 3 (Article 6 (1) (a)); those who may 'according to criminal intelligence or other evidentiary circumstances' commit such an offence (Article 6 (1) (b)); or those who fall under neither category but where 'there are factual reasons to believe that an exchange of information and intelligence . . . could assist in detecting preventing or investigating a crime' involving one of the offences listed under Article 4 (a) of the Decision (Article 6 (1) (c)).

Article 7 (1) provides that the SIRENE bureaux or Europol or 'any other framework established at bilateral or multilateral level among the Member States' may be used to exchange information and intelligence under the Decision.

Article 9 stipulates that when existing channels of communication are used the data protection rules that apply to those channels – such as those found in the Europol Convention – should also apply to exchanges that take place under this Decision.

Article 9 (2) stipulates that if other channels are used 'equivalent standards of data protection' should apply.

General Remarks

This Framework Decision, if implemented, would continue an established pattern in EU policy in this area. Cooperation between law enforcement authorities is considered an important if not crucial aspect in the fight against crime and terrorism. Cultural, organizational and legal barriers preventing data exchange need to be addressed. Many initiatives including the draft Framework Decision result in a significant increase in the exchange of information for the purposes of law enforcement, with much more personal data being exchanged between Member States. Although data exchange in itself might be necessary in the fight against crime and terrorism, the range of offences covered by the Decision is broad and goes far beyond the relatively narrow range of offences covered by other EU instruments, such as the Europol Convention. The categories of person on whom data may be exchanged is also broad; Article 6 (c) in particular is unclear and could result in widespread data exchange on individuals not suspected of any crime. There ought to be clear criteria for determining when personal data may be exchanged.

The draft Framework Decision introduces an obligation to exchange information when available. Given the potentially far-reaching implications of this development, we would stress the importance of examining whether the proposal is proportionate. The fight against terrorism is increasingly being used as the justification for new initiatives in this field, but many go far beyond this purpose. It is important to recognise that a derogation from fundamental rights that might be justified to tackle terrorism will not necessarily be justified where other criminal activity is concerned.

By introducing the principle that data must be exchanged when available, a link is established with The Hague Programme,² which introduces the availability principle. The Hague Programme sets out strict conditions to be observed when applying the availability

² Presidency Conclusions 4/5 November 2004 (14292/04) Annex 1: The Hague Programme

principle such as the need to protect sources of information and the confidentiality of data, the need to guarantee the integrity of the data to be exchanged, the supervision of respect for data protection and appropriate control prior to and after the exchange. The draft Framework Decision, however, does not match those strict conditions and it is therefore necessary to develop these conditions in the Decision.

According to the draft Decision, existing channels of communication should be used for data exchange, and existing rules on data protection should apply. However, it is not that straightforward. There are differences between the data protection rules that apply under Schengen and those that apply to Europol, for example. Moreover, rules have not yet been harmonised throughout the EU. The rules that apply to the SIRENE bureaux are found in the national laws of each Member State; they have not been harmonised. This can lead to discrepancies, and a situation might well arise where data are retained in a receiving Member State for longer than they would have been retained in the originating Member State. In order to avoid such complications, and in the interests of clarity, the data protection rules applicable to data exchange under this Decision ought to be contained within the text of the Decision itself. As well as addressing issues of retention, data quality, security and control, these rules should make it clear who is responsible for the further processing of personal data exchanged under the Decision. A specific set of data protection rules is available in the position paper on Law Enforcement & Information Exchange in the EU adopted by the Conference in Krakow.

Conclusion

To provide for all the necessary guarantees for an adequate level of data protection in conformity with the existing legal framework, the Conference recommends that the draft Framework Decision should be amended, taking into account the Krakow Declaration of 25-26 April 2005 and the remarks made in this opinion.