Fight against terrorism: processing and protection of personal data in the framework of police and judicial cooperation in criminal matters. Framework Decision

2005/0202(CNS) - 25/01/2012 - Follow-up document

The Commission presents a report taking stock of the state of implementation of Council Framework Decision 2008/977/JHA on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters.

The main points of the report are as follows:

Scope of national implementation measures: the Framework Decision applies only to the processing of personal data transmitted or made available between Member States (Article 1(2)). Processing personal data by police and justice in criminal matters at national level does not fall within the scope of the Framework Decision.

Three Member States considered the limited scope of the Framework Decision as problematic. Italy and the Netherlands reported difficulties in distinguishing in practice between cross-border processing of data under Framework Decision 2008/977 and processing at national level, and the related complexity for law enforcement authorities in Member States to cope with different processing rules for the same personal data. Poland pointed to the deficiencies of the Framework Decision in general and, in particular, stressed its support for the Commission's aim to establish a comprehensive framework and the extension of general data protection rules to the area of police and judicial cooperation in criminal matters.

Information to data subjects (Article 16): under the Framework Decision, Member States must ensure that their competent authorities inform data subjects that their data are being processed or transmitted to another Member

State. Almost all Member States indicated that they provide data subjects with some information on the processing of their personal data. France indicated that it does not do so. Denmark does not grant this right either, but reported that the controller must keep a register and inform the public.

The right of information is subject to limitations in the vast majority of Member States.

The Netherlands stated that a general obligation to inform the data subject was not entirely consistent with the nature of the work of the police and judiciary, but that certain arrangements are in place to make sufficient provision for informing the data subject as required on data processing by the police and judicial authorities.

The Netherlands also stated that this provision need not be implemented because Article 16(1) merely refers to national laws of Member States.

The Framework Decision establishes data subjects’ right to information but does not contain any details on the methods or on possible exemptions. Even if, according to the Member States, the right to information is generally granted, implementation varies considerably.

Right of access of data subjects (Article 17): the Framework Decision contains general rules providing data subjects with the right to access their data. It does not specify in detail what kind of information needs to be given to the data subject. It also leaves it to Member States to decide whether data subjects may exercise their right of access directly or whether they must use the indirect route.

All Member States grant some form of right of access to data subjects. Equally, all Member States provide for exemptions from the right of access. The most frequently mentioned reasons for not granting the right of access include the prevention, investigation and prosecution of criminal offences and national security, defence and public security.

Other issues raised by Member States: 6 Member States made comments on issues of concern to them:

- Poland considered that the Framework Decision contained numerous deficiencies, which should be remedied, and expressed support for reform in order to establish a comprehensive and coherent data protection system at EU level;

- Italy and the Netherlands raised a difficulty in distinguishing in practice between cross-border processing of data under Framework Decision 2008/977 and processing at national level, and the related difficulty for law enforcement authorities in Member States to cope with different processing rules for the same personal data;

- Italy, the Czech Republic and the Netherlands expressed criticism towards the rules on international transfers included in the Framework Decision. In particular, Italy said that it was necessary to provide for an adequate and more uniform level of data protection for data transfers to third countries. The Netherlands considered problematic the lack of criteria in the Framework Decision to determine the adequate level of protection of a third country, leading to variable implementation by Member States. The Czech Republic considered the rules on international transfers in the Framework Decision as 'unrealistic';

- France referred to a specific problem at national level in relation to the storage periods of personal data transmitted to and from a third country having different requirements in that respect;

- Slovakia said it was necessary to differentiate more between data processing by the police and by the judiciary (court proceedings);

- the Czech Republic and the Netherlands indicated that it was confusing for law enforcement to have to comply with multiple data protection rules at international (such as the Council of Europe), EU and national level.

The report considers that the practical difficulties encountered by a number of Member States in distinguishing between rules for domestic and cross-border data processing, **could be solved through a single set of rules covering data processing both at national level and in a cross-border context.** The scope and possible exemptions at EU level regarding the data subjects' right to information would merit further clarification. **Minimum harmonised criteria regarding data subjects' right of access** could strengthen the rights of data subjects while also providing exemptions to allow the police and justice to properly perform their tasks.

Under Article 16 of the Treaty on the Functioning of the European Union, which enshrines the right to the protection of personal data, there is now the possibility of establishing a comprehensive data protection framework ensuring both a high level of protection of individuals' data in the area of police and judicial cooperation in criminal matters and a smoother exchange of personal data between Member States' police and judicial authorities, fully respecting the principle of subsidiarity.