EUROPEAN COMMISSION

Brussels, 25.1.2012
COM(2012) 12 final

REPORT FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS

based on Article 29 (2) of the Council Framework Decision of 27 November 2008 on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters

{SEC(2012) 75 final}

REPORT FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS

based on Article 29 (2) of the Council Framework Decision of 27 November 2008 on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters

1. INTRODUCTION

1.1. Background

Council Framework Decision 2008/977/JHA of 27 November 2008[1] (hereafter 'Framework Decision') on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters puts in place a general legislative framework for data protection on police and judicial cooperation in criminal matters. It entered into force on 19 January 2009[2].

The Framework Decision was necessary as at that time there was no general instrument at European level covering data processing in the areas of police and judicial cooperation in criminal matters[3]. Article 3 of Directive 95/46/EC on the protection of personal data and on the free movement of such data states that it does not apply 'to the processing of personal data in the course of an activity which falls outside the scope of Community law, such as those provided for by Title VI of the Treaty on European Union, nor, in any case, to processing operations concerning public security, defence, state security or the activities of the State in areas of criminal law'.

The purpose of the Framework Decision is to provide at EU level a high level of protection of the fundamental rights and freedoms of natural persons when processing personal data in the framework of police and judicial cooperation in criminal matters. At the same time, a high level of public safety should be guaranteed[4]. It does not preclude Member States from providing higher safeguards to protect personal data collected or processed at national level[5].

The scope[6] of the Framework Decision is limited to the processing of personal data for the purpose of preventing, investigating, detecting or prosecuting criminal offences or executing criminal penalties of data which are or have been transmitted or made available:

- between Member States,

---

1 OJ L 350, 30.12.2008, p. 60.

2 Article 30.

3 Recital 5 of 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, OJ L 281, 23.11.1995, p. 31.

4 Article 1.

5 Article 1(5).

6 Article 1(2).

- by Member States to authorities or information systems established on the basis of Title VI of the Treaty on European Union ('Police and judicial cooperation in criminal matters'); or

- to the competent authorities of the Member States by authorities or information systems established on the basis of the Treaty on European Union or the Treaty establishing the European Community.

Personal data which have been transferred from one Member State to another one may also be transferred to third States or international bodies, provided that certain requirements are met[7].

The Framework Decision fully applies to the UK and Ireland, because it is a development of the Schengen *acquis*. The United Kingdom and Ireland are parties to the Framework Decision in accordance with Article 5 of the Protocol integrating the Schengen *acquis* into the framework of the European Union annexed to the Treaty on European Union and to the Treaty establishing the European Community, and Council Decisions 2000/365/EC and 2002/192/EC.

As regards Iceland, Norway, Switzerland and Liechtenstein, the Framework Decision constitutes a development of the Schengen *acquis* within the meaning of the Agreement and the Protocols concluded by either the Council of the European Union or the European Union with Iceland and Norway, the Swiss Confederation and Liechtenstein, and Council Decisions 1999/437/EC, 2008/149/JHA and 2008/262/JHA.

1.2. Content of Framework Decision 2008/977/JHA

The **scope** of the Framework Decision does not cover domestic processing of personal data by the competent judicial or police authorities in the Member States (Article 1 (2)).

In general, the sector-specific legislative instruments for police and judicial cooperation in criminal matters that contain provisions on the protection of personal data and that had been adopted **prior** to the date of entry into force of the Framework Decision take precedence over the latter (Article 28). Instruments deemed to set out 'complete and coherent set of rules' regarding data protection are not affected by the Framework Decision (recital 39). Other sector-specific measures that contain data protection rules of a more limited scope take precedence over the Framework Decision only if these rules are more restrictive than the latter. Otherwise the Framework Decision applies (recital 40).

The Framework Decision specifies the objectives of data protection in the framework of police and judicial activities. It lays down rules on the lawfulness of processing personal data to ensure that any information that might be exchanged is processed lawfully and in accordance with the fundamental principles of data quality.

It also defines the rights of data subjects to ensure the protection of personal data without jeopardising the interests of criminal investigations. To this end, the data subjects must be informed and must have access to their personal data.

National supervisory authorities, acting in complete independence in exercising the functions entrusted to them, must advise and monitor the application of the measures adopted by the Member States to transpose the Framework Decision.

---

[7] Article 13.

1.3. The Commission's obligation to report on implementation

Under Article 29(1) of the Framework Decision, the Member States must take measures to comply with this Decision before 27 November 2010.

According to Article 29(2), they must 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, as well as information on the supervisory authorities referred to in Article 25 of the Framework Decision.

The Commission must prepare a report using the information submitted by the Member States. The Council must, before 27 November 2011, assess the extent to which Member States have complied with this Framework Decision.

1.4. Information sources on which this report is based

By **9 November 2011,** 26 out of 27 Member States, as well as Liechtenstein, Norway, Iceland and Switzerland, had sent the Commission information on the implementation of the Framework Decision.

Of these **26** Member States, **14** Member States indicated that their legislation in force implements the Framework Decision (Belgium, Czech Republic, Denmark, Germany, Estonia, Ireland, Hungary, Latvia, Lithuania, Luxembourg, Austria, Slovakia, Sweden, and United Kingdom). Germany, Ireland, Estonia and Sweden stated that they were still investigating whether there was a need for further implementation measures.

9 Member States can be considered to have implemented the Framework Decision partially, as they report that implementing legislation still needs to be adopted.

4 Member States have either not reacted to the Commission's request for information (Romania) or indicated that they have not implemented the Framework Decision (Greece, Italy[8], Cyprus).

The content of the information, particularly the level of detail, provided by the Member States in response to the Commission questionnaire varies. Table 1 provides an overview of replies: it mirrors Member States' assessment of the status of implementation of the Framework Decision.

2. TRANSPOSITION OF THE FRAMEWORK DECISION

2.1. Framework Decision ex-Article 34(2)(b) of the Treaty on European Union

This Framework Decision is based on the Treaty establishing the European Union (TEU), and in particular Articles 30, 31(e), and Article 34(2)(b) thereof.

[8] **Italy** informed the Commission that specific implementing instruments have not yet been formally adopted. It refers to the Personal Data Protection Code[8], the Criminal procedure Code and other acts which contain provisions applicable to processing in these areas. Other Member States take a different approach and indicate that the data protection rules in force also apply to the processing of personal data by Police and Justice at national level as well as to the cross-border processing by Police and Justice in criminal matters. In addition they have informed the Commission of additional implementing measures that are currently being prepared.

Framework Decisions as legal instruments can best be compared to a directive, as they are binding upon Member States as to the result to be achieved but leave to the national authorities the choice of form and methods. However, framework decisions do not have direct effect[9].

On the basis of Article 10 of the Protocol on transitional provisions concerning acts adopted on the basis of Titles V and VI of the TEU prior to the entry into force of the Treaty of Lisbon (No 36), annexed to the Treaties, Commission powers under Article 258 of the TFEU are not applicable (and those of the ECJ remain limited) in respect of 'ex-third pillar' acts for a transitional period of five years from the entry into force of the Lisbon Treaty (i.e. until 1 December 2014).

Below are some details on the implementation of four key provisions of the Framework Decision as reported by the Member States in response to the Commission's request of 9 December 2010.

2.1.1. 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.

Table 2 of the Annex provides an overview of the implementing measures in the Member States. Most Member States referred to the general data protection legislation as one of the implementing measures of the Framework Decision and added a reference to applicable sectoral legislation for police, justice, customs and tax authorities. Some Member States decided not to adopt legislative instruments, but to implement the Decision by issuing administrative circulars (e.g. Germany and the United Kingdom).

Most Member States indicated that **general data protection legislation applies to the processing of personal data by the police and justice both at national level and in a cross-border context[10], however often alongside Criminal Procedure Acts and Police (Data) Acts[11].** Thirteen Member States (Belgium, Czech Republic, Germany, Estonia, Italy, Luxembourg, Hungary, Malta, the Netherlands, Slovenia, Slovakia, Finland and Sweden) referred to Criminal Procedures Acts or similar legislation. Seven Member States (Czech Republic, Germany, Hungary, the Netherlands, Slovenia, Finland and Sweden) reported the existence of a specific Police (Data) Act[12]. Three Member States (e.g. Bulgaria, Portugal, Lithuania) added that they had also adopted specific legislation to implement certain provisions of the Framework Decision not covered by the general legislation, which only apply to cross-border processing of personal data[13].

---

9 See Case C-105/03, Pupino, judgment of 16.5.2005, para. 34, 43-45, 47, 61, in which the ECJ held that national courts interpreting national laws are obliged to strive to achieve a consistent interpretation, including framework decisions.

10 This was already the case before the adoption of the Framework Decision (see Commission Staff Working Document, Impact Assessment, SEC(2005) 1241 of 4.10.2005, point 5.1.2.).

11 See Table 2.

12 See Table 2.

13 See comments from the Netherlands.

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 their support to 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.[14]

2.1.2. Information of data subjects (Article 16, recitals 26-27)

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 for the purpose of prevention, investigation, detection and prosecution of criminal offences or the execution of criminal penalties. The form, content, method and the exceptions (i.e. no provision or limited provision of information) used to do so should be determined under national law. This may take a general form, by passing a law or publishing a list of the processing operations. If data are transferred to another Member State, each Member State may request the other Member State not to inform the data subject.

Table 3 shows that **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.** National legislation either limits this right for the purpose of preventing, investigating, detecting and prosecuting criminal offences or provides that data processing by specific data controllers (police and/or judiciary) is exempted from application of this right. In some cases, limitations/exemptions are laid down without specifying for which activities. A considerable number of Member States report such limitations for police, military police, courts, customs and tax authorities.

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 (i.e. laws inform about cases and conditions of data processing; the public prosecutor informs the data subject of exercise of special investigative powers, if the interests of the investigation permit). 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.

---

[14] See also the contribution of Poland (Ministry of Interior) to the public consultation launched by the Commission end 2010 (referred to in their reply to the questionnaire): http://ec.europa.eu/justice/news/consulting_public/0006/contributions/public_authorities/pl_min_pl.pdf.

2.1.3. Right of access of data subjects (Article 17)

The Framework Decision provides that a data subject has the right to obtain, without constraint, excessive delay or expense, either:

(a) at least a confirmation from the controller or from the national supervisory authority as to whether or not data relating to him have been transmitted or made available and information on the recipients or categories of recipients to whom the data have been disclosed and communication of the data undergoing processing, or

(b) at least a confirmation from the national supervisory authority that all applicable checks have been carried out.

Member States may legislate restrictions to this right of access, in order to avoid obstructing official or legal inquiries, investigations or procedures; prejudicing the prevention, detection, investigation and prosecution of criminal offences or for the execution of criminal penalties; protecting public security; protecting national security; and protecting the data subject or the rights and freedoms of others (Article 17(2)). Any refusals by the controller to provide this information must be made in writing (Article 17(3)).

The information provided by the Member States and compiled in Table 4 on the right to access mirrors the situation as regards giving information to the data subject. It can be concluded that **all Member States[15] grant some form of right of access to data subjects**. This right is generally enshrined in the country's general data protection legislation. Many Member States also regulate details of the access right in sector-specific legislation (such as the Police Acts).

Equally, all Member States provide for **exemptions from the right of access**. The most frequently mentioned reasons for not granting the right of access are:

– to prevent, investigate, detect and prosecute criminal offences;

– national security, defence and public security;

– economic and financial interests of a Member State and of the EU (including monetary, budgetary and taxation matters)[16];

– to protect the rights and freedoms of the data subject or other persons.

Concerning the **way in which access to personal data is granted**, some Member States have addressed this issue explicitly, others have not. Some Member States indicated that they grant data subjects the right to send a request for access to their data directly to the competent authority (i.e. Austria, Germany, Bulgaria, Finland, Ireland, Latvia, Malta, Netherlands, Poland, Slovakia, Sweden, United Kingdom) while others only allow for 'indirect' access (Belgium, France). In the latter case, it is the national supervisory authority instead of the data subject that has access to all personal data related to the data subject. In Finland and Lithuania, data subjects are given a choice. In Portugal, direct access is the general rule, but indirect access is provided for in cases where the processing of personal data has a bearing on

---

15 This conclusion can be drawn although some Member States did not provide specifications (see details in Table 3).

16 This is not an exemption that is expressly mentioned in Article 17 of Framework Decision 2008/977. It does, however, reflect an exemption listed in Article 13(1) of Directive 95/46/EC.

state security or the prevention or investigation of crime. The situation is similar in Luxembourg, where generally access is granted directly, but if an exemption applies, the request for access must be addressed to the data protection supervisory authority.

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.

2.1.4. National Supervisory authorities (Article 25)

Framework Decision 2008/977 recognises that the establishment in Member States of supervisory authorities, exercising their functions with complete independence, is 'an essential component of the protection of personal data processed within the framework of police and judicial cooperation between the Member States' (recital 33). It also states that the supervisory authorities already established in Member States under the Directive 'should also be able' to assume such responsibility (recital 34). Article 25 of Framework Decision 2008/977 mirrors an important part of the provision on the supervisory authorities of Article 28 (paragraphs 1-4, 7) in Directive 95/46/EC concerning the powers of the authority, its obligation to act in complete independence and the duty of professional secrecy. Each authority must be endowed with a number of powers, comprising investigative powers (including access to data and collection of necessary information), effective powers of intervention (such as issuing and publishing opinions before processing operations; ordering blocking, erasure or destruction of data; imposing a temporary or definitive ban on processing; warning or admonishing the controller; referring the matter to national parliaments or other political institutions) and the power to engage in legal proceedings.

Table 5 shows that, in most cases, the national supervisory authorities in charge of monitoring the implementation and application of the general data protection rules are also responsible for supervising the implementation and application of Framework Decision 2008/977.

Sweden indicated that its Data Inspection Board still needs to be designated as the competent supervisory authority under Article 25 of the Framework Decision.

Some Member States expressly raised the issue of supervision of data processing by the judiciary[17]. Denmark indicated that the Court Administration is responsible for supervising data processing by the judiciary and Austria noted that the data protection supervisory authority is not competent to decide on complaints for violation of data protection rules by the judiciary. In Luxembourg the supervision of data processing is generally the competence of the Data Protection Commission. Processing activities carried out in the framework of a national provision implementing an international convention are supervised by an authority which is composed of the *Procureur Général d'Etat* or his delegate and two members of the Data Protection Commission proposed by the latter and appointed by the Minister.

2.1.5. Other issues raised by Member States

Out of the 26 Member States, 20 – 8 of which did not reply at all to this question (Belgium, Denmark, Estonia, Greece, Hungary, Luxembourg, Cyprus and Austria) – did not report any

[17] See recital 35, last sentence, of the Framework Decision, stating that the powers of supervisory authorities 'should not interfere with specific rules set out for criminal proceedings or the independence of the judiciary'.

particular problems with the Framework Decision. .. As shown in Table 6, 6 Member States made comments on issues of concern to them, such as the following issues:

- 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. Finally, 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);

- Both 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.

3. THE WORK AHEAD

This report takes stock of the state of implementation and functioning of the Framework Decision on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters.

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.