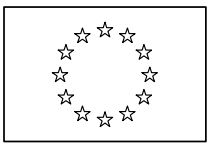

COMMISSION OF THE EUROPEAN COMMUNITIES

Brussels, 7.3.2007
COM(2007) 87 final

COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL

on the follow-up of the Work Programme for better implementation of the Data Protection Directive

COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL

on the follow-up of the Work Programme for better implementation of the Data Protection Directive

(Text with EEA relevance)

Directive 95/46/EC[1] set a milestone in the history of the protection of personal data as a fundamental right, down the path paved by Council of Europe Convention 108[2]. Pursuant to Article 33 of the Directive, the Commission's First report on its implementation[3] concluded that, although no legislative changes were needed, work had to be done and that there was considerable scope for improvement in implementing the Directive.

The report contained a *Work Programme for better implementation of the data protection Directive*. This Communication examines the work conducted under this programme, assesses the present situation, and outlines the prospects for the future as a condition for success in a number of policy areas in the light of Article 8 of the European Charter of Fundamental Rights, recognising an autonomous right to the protection of personal data.

The Commission considers that the Directive lays down a general legal framework that is substantially appropriate and technologically neutral. The harmonised set of rules ensuring a high standard of protection for personal data throughout the EU has brought considerable benefits for citizens, business and authorities. It protects individuals against general surveillance or undue discrimination on the basis of the information others hold on them. The trust of consumers that personal details they provide in their transactions will not be misused is a condition for the development of e-commerce. Business operate and administrations co-operate throughout the Community without fearing that their international activities be disrupted because personal data they need to exchange are not protected at the origin or the destination.

The Commission will continue to monitor the implementation of the Directive, work with all stakeholders to further reduce national divergences, and study the need for sector-specific legislation to apply data protection principles to new technologies and to satisfy public security needs.

---

1 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 No. L 281, 23.11.1995, p. 31, henceforth "the Directive".

2 ETS No. 108; henceforth “Convention 108”

3 First report on the implementation of the Data Protection Directive (95/46/EC), COM (2003) 265 final, of 15.5.2003

1. THE PAST: ACHIEVEMENTS UNDER THE WORK PROGRAMME

Since publication of the first report work has been carried out in the following 10 action areas[4].

Action 1 : Discussions with Member States and Data Protection Authorities

The Commission has been conducting a "structured dialogue" with Member States on national transposition. This includes a detailed analysis of national legislation and discussions with national authorities aimed at bringing national legislation fully in line with the requirements of the Directive.

Action 2 : Association of the candidate countries with efforts to achieve a better and more uniform implementation of the Directive

Representatives of these Member States attended meetings of the committee of Member State representatives set up by Article 31 of the Directive ahead of accession, as they had been doing with the Article 29 Working Party[5] since 2002. The Commission has meanwhile been working closely with their Authorities in the process of adopting national legislation, providing guidance for alignment with the acquis in order to keep formal infringement procedures to a minimum.

Action 3 : Improving the notification of all legal acts transposing the Directive and notifications of authorisations granted under Article 26(2) of the Directive

The structured dialogue conducted under Action 1 has given the Commission a clearer and comprehensive picture of national measures implementing the Directive, including secondary and sector-related legislation. The Commission, in a letter sent to Member States in August 2003, proposed common criteria to deal pragmatically with notifications under Article 26(3) of the Directive. This has resulted in an increase in notifications from some Member States. The exchange of best practices and knowledge between national authorities has been enhanced by making public on the Commission's website a selection of key national policy papers, decisions and recommendations.

Action 4 : Enforcement

In its Declaration on Enforcement, the Working Party agreed on the principle of EU-wide, synchronized national enforcement actions, setting criteria to identify issues for investigations. In March 2006 the national Data Protection Authorities launched a joint investigation on the processing of personal data in the private health insurance sector.

Action 5 : Notification and publicising of processing operations

The Working Party has produced a report on this issue, outlining current national situations and making recommendations along the same lines as the Commission. This has been followed by the Vademecum on Notification Requirements, conceived to provide a

---

4 The Commission's first report, as well as publicly available documents adopted under the Work Programme mentioned here can be found at http://ec.europa.eu/justice_home/fsj/privacy/lawreport/index_en.htm

5 Working Party on the Protection of Individuals with regard to the processing of Personal Data set up by Article 29 of the Directive, henceforth "the Working Party"

comprehensive view of the different national rules, as well as practice and guidance to the data controllers.

Action 6 : More harmonised information provisions

In addition to the Commission's analysis of national legislation under the structured dialogue, the Working Party has recognised the need for harmonisation and sought a common approach for a pragmatic solution. It has provided guidelines for controllers on relevant concrete cases, on content and form of the information, and on models for multi-layered privacy notices or an information notice on transfer of PNR data.

Action 7 : Simplification of the requirements for international transfers

a) a more extensive use of findings of adequate protection in respect of third countries under Article 25(6)

The Commission has adopted a number of adequacy findings since the publication of the Work Programme. Argentina, Guernsey and the Isle of Man have been declared to guarantee an adequate level of protection.

The Commission has also reviewed the functioning of adequacy decisions previously adopted. A Commission services' report was presented in 2004 on the functioning of the Safe Harbour, followed by an informative notice and a standard form to lodge complaints with the data protection panel. This work has been followed by a far-reaching Conference on International Transfers of Personal Data organised in October 2006 jointly with the Working Party and the US Department of Commerce. The application of the adequacy findings on Switzerland and Canada has also been assessed.

b) further decisions on the basis of Article 26(4) so that economic operators have a wider choice of standard contractual clauses

The Commission adopted a decision recognising an additional set of contractual clauses to provide adequate safeguards for transfers of data to controllers in third countries. These clauses were proposed by a group of representative business associations, including the International Chamber of Commerce. The Commission services also presented a first report on the implementation of the previous Commission decisions on contractual clauses in 2006.

c) the role of binding (intra) corporate rules in providing adequate safeguards for intra-group transfers of personal data;

After preparatory work in 2003 and 2004, two key documents were adopted by the Working Party. One sets out a co-operation procedure among national supervisory authorities to issue common opinions on adequate safeguards resulting from the "Binding Corporate Rules". The other establishes a model checklist to be used by data controllers to apply for approval of those rules as providing adequate safeguards.

d) a more uniform interpretation of Article 26(1) of the Directive

The Working Party adopted an Opinion laying down important elements for guidance on the use of the exemptions to the principle of adequate protection in third countries.

Action 8 : Promotion of Privacy Enhancing Technologies

Work in 2003 and 2004 by the Commission and the Working Party has focussed in the forthcoming Commission Communication on Privacy Enhancing Technologies (PETs), setting out future policy.

Action 9 : Promotion of self-regulation and European Codes of Conducts

The Working Party approved the European code of conduct of the Federation of European Direct Marketing (FEDMA); an important milestone. Regrettably, other attempts have not materialised into similar codes fulfilling criteria of comparable quality. The European social partners unfortunately also failed to conclude a European agreement on the protection of personal data in the employment context, despite earlier progress.

Action 10 : Awareness raising

A Eurobarometer survey was conducted into European citizens' and companies' views about privacy. It broadly shows that people are concerned about privacy issues, but not sufficiently aware of the existing rules and mechanisms to protect their rights.

2. THE PRESENT: OVERVIEW OF IMPLEMENTATION OF THE DIRECTIVE

Implementation has improved

All Member States have now transposed the Directive. On the whole, national transposition covers all the main provisions along the lines of the Directive.

The actions undertaken under the Work Programme have been positive and have substantially contributed to improving the implementation of the Directive throughout the Community. The decisive involvement of the national data protection supervisory authorities through their participation in the Working Party has played a major role.

But some countries have not yet properly implemented.

Following the work carried out in preparing the Commission's first report in 2003, the thorough analysis of national data protection legislation under the structured dialogue has illuminated the way the Directive has been transposed throughout the Community. It has clarified a number of legal issues and doubts about the coherence of certain national provisions and practices with the rules of the Directive.

The structured dialogue has also shown that some Member States have failed to incorporate a number of important provisions of the Directive. In other cases, transposition or practice has not been conducted in line with the Directive or has fallen outside the margin of manoeuvre left to Member States.

One concern is respect for the requirement that data protection supervisory authorities act in complete independence and are endowed with sufficient powers and resources to exercise their tasks. These authorities are key building blocks in the system of protection conceived by the Directive, and any failure to ensure their independence and powers has a wide-ranging negative impact on the enforcement of the data protection legislation.

The Commission is conducting a comparative analysis of all the cases where wrong or incomplete transposition is suspected, in order to ensure a coherent approach. Some Member States have acknowledged the existence of their legislative shortcomings and have committed themselves to introducing the necessary corrections, something the Commission strongly encourages. Other problematic issues have been raised in complaints by citizens. Where a breach of Community Law remains, the Commission, as guardian of the Treaties, will open formal infringement procedures against the Member States concerned, in accordance with Article 226 EC. A number of such proceedings have already been opened.

In some case divergences arise within the margin of manoeuvre of the Directive

The Directive contains a number of provisions that are broadly formulated and, explicitly or implicitly, leave Member States a margin of manoeuvre in adopting national legislation. Within those limits differences in national legislation may arise[6]. Such divergences are no greater in this sector than in other fields of economic activity and are a natural consequence of such a margin.

But those divergences do not pose a real problem to the internal market

The Commission ordered a study to conduct an "Economic evaluation of the Data Protection Directive (95/46/EC)[7]" to measure the Directive's economic impact on data controllers. Focusing on a number of selected cases, the study shows that despite some divergences, the Directive has been implemented with modest costs for firms.

A greater degree of convergence would certainly be desirable to promote positive initiatives like simplification, self-regulation or the use of binding corporate rules. However, no evidence is found among the complaints received by the Commission that national divergences within the limits of the Directive may actually obstruct the proper functioning of the internal market or limit the free flow of data on grounds of a lack or inadequacy of protection in the country of origin or destination. Nor do constraints within their country of establishment distort competition between private operators. National divergences do not prevent enterprises from operating or establishing themselves in different Member States. And they do not call into question the commitment of the European Union and its Member States to the protection of fundamental rights.

The Directive is therefore fulfilling its objectives: to secure the free flow of personal data within the internal market while ensuring a high level of protection in the Community.

The rules themselves are substantially appropriate

A different question is whether the legal solutions provided by the Directive, beyond achieving harmonisation, are themselves appropriate to the issues at stake.

Some provisions have been criticised. It has been argued that notification imposes a burden, but it has considerable value as a transparency measure for data subjects, an awareness-raising exercise for data controllers and a monitoring tool for authorities. The Internet, and new possibilities for data subjects to interact and to access services provided in third countries raise questions on the rules for determining the applicable national law or for transfers of data

---

6 Recital (9) of the Directive

7 http://ec.europa.eu/justice_home/fsj/privacy/docs/studies/economic_evaluation_en.pdf

to third countries, issues to which case law has given only a partial answer[8]. RFID (Radio Frequency IDentification) devices raise fundamental issues on the scope of the data protection rules and the concept of personal data. The combination of sound and image data with automatic recognition imposes particular care when applying the principles of the Directive.

A similar debate has taken place in the Council of Europe concerning the relevance in today's world of the principles contained in Convention 108. There is a general understanding that those principles remain valid and provide a satisfactory solution.

Adapting to evolution in technology

The Commission considers that the Directive is technologically neutral and that its principles and provisions are sufficiently general, that its rules may continue to apply appropriately to new technologies and situations. It may be necessary, though, to translate those general rules into particular guidelines or provisions to take account of the specificities involved in those technologies.

Accordingly, Directive 2002/58/EC particularises and complements Directive 95/46/EC with respect to the processing of personal data in the electronic communication sector, ensuring the free movement of such data and of electronic communication equipment and services in the Community. This Directive is currently being reviewed as part of the overall review of the regulatory framework for electronic communications.

Considerable effort has been invested by the Working Party on technological matters, such as unsolicited communications ('spam'), email filters, and the processing of traffic data for billing purposes or of location data for the purpose of value-added services. RFID technology has been the subject of a series of workshops and a public consultation by the Commission services to discuss the privacy and security issues raised.

Considering the requirements imposed by public interests

The articulation in the Directive between the protection of the individual's fundamental rights and freedoms and the needs imposed by public interests is determined by two types of provision.

One type of provision excludes a number of matters from the scope of the Directive, such as Article 3 with regard to "*public security, defence, State security (including the economic well-being of the State when the processing operations relates to State security matters) and the activities of the State in areas of criminal law*". The Court of Justice has made clear that processing for safeguarding public security and for law-enforcement purposes does not fall within the scope of the Directive[9]. In view of the need for a common set of EU data protection rules the Commission has adopted a proposal on the protection of personal data processed in the framework of police and judicial co-operation in criminal matters[10], to accompany its proposal on the exchange of information under the principle of availability[11]. In this area the

---

8 Case C-101/01 ("Lindqvist"), judgment of 6 November 2003

9 Joined Cases C-317/04 and C-318/04 ("PNR"), judgment of 30 May 2006

10 COM(2005) 475 final of 4.10.2005

11 COM(2005) 490 final of 12.10.2005

EU has concluded an International Agreement with the US to address the use of passengers' PNR data to fight crime[12].

A second type of provision provides that Member States may restrict data protection principles under certain circumstances, as in Article 13, "*when such a restriction constitutes a necessary measure to safeguard* [the list of important public interests which follows]". Such restrictions may take account, for example, of the need to fight crime or to protect public health in emergencies. Other provisions of the Directive contain a similar possibility for limited exceptions. The Court of Justice has made clear that data originally collected for "commercial purposes" may only be subsequently used for a different, public interest purpose according to the conditions set out in this Article. Furthermore, the limits imposed on the national legislator are equivalent to those set by Article 8 of the European Convention on Human Rights, and the case law of the European Court of Human Rights is of paramount importance. [13]. This mechanism, open to Member States' appreciation of what may constitute "*a necessary measure*" and an "*important public interest*" is, by its very nature, a major source of discrepancy among national legislations.

Harmonisation of such restrictions has only been carried out in a limited number of sectors, a recent example being the data retention Directive 2006/24/EC[14], for which the Commission has announced its intention to set up an expert group, in order to discuss difficulties such as the implementation of the Directive into national law.

While giving substance to the fundamental right

The Commission is committed to respecting the Charter of Fundamental Rights in all its proposals. Regarding the right to the protection of personal data in Article 8 thereof, the Directive sets a high standard and serves as a point of reference for ensuring coherence with the respect for privacy in all Community legislation in different fields.

3. THE FUTURE: THE ROAD AHEAD

With this situation in the background, the Commission intends to pursue a policy characterized by the following elements.

The ratification of the Constitutional treaty may open new perspectives

The Constitutional Treaty would have an enormous impact in this field. It would enshrine in Article II-68 the right to protection of personal data in Article 8 of the Charter of Fundamental Rights. It would also create a specific and self-standing legal basis for the Union to legislate in this matter in Article I-51, paving the way for adopting instruments applicable in all sectors. The present division into "pillars" and the limitations of Article 3 of the Directive would no longer be at issue. However, until the situation concerning the ratification process of the Constitutional Treaty becomes clearer the Commission has stressed the need for more efficient procedures in the area of Freedom, Security and Justice under the current Treaties[15].

---

12 OJ L 298, 27.10.2006, p. 29

13 Joined Cases C-465/00, C-138/01 and C-139/01 ("Rechnungshof"), judgment of 20 May 2003

14 OJ L 105, 13.4.2006, p. 54

15 COM(2006) 331 final of 28.6.2006

The Directive should not be amended

For the reasons set out above, the Commission considers that the Data Protection Directive constitutes a general legal framework which fulfils its original objectives by constituting a sufficient guarantee for the functioning of the Internal Market while ensuring a high level of protection. It gives shape to the fundamental right to protection of personal data; respect of its rules should ensure trust of the individuals on the way their information is used, a key condition for the development of the e-economy; it sets a benchmark for initiatives in a number of policy areas; it is technologically neutral and continues to provides solid and appropriate responses to these issues.

Therefore, the Commission does not envisage submitting any legislative proposal to amend the Directive.

The Commission will pursue proper implementation of its provisions at national and international level

Some of the inconsistencies in national legislation result from incorrect or incomplete transposition of the provisions of the Directive. On the basis of the information gathered in the structured dialogue with Member States, together with that collected as a result of complaints received from citizens, the Commission will continue to work with Member States, and, where necessary, will launch official infringement procedures, so as to ensure a common playing field for all Member States.

The Commission also urges Member States to ensure proper implementation of national legislation adopted pursuant to the Directive. At the same time, it will continue to monitor and contribute to developments on international fora, such as the Council of Europe, OECD and the UNO, to ensure coherence of Member States' commitments with their obligations under the Directive.

The Commission will produce an interpretative communication on some provisions

The problems identified in implementing particular provisions of the Directive that may lead to formal infringement procedures correspond to an understanding by the Commission about the meaning of the provisions in the Directive and about the correct way to implement them, taking into account the case law, as well as the interpretation work conducted by the Working Party.

Such ideas will be clearly set forth in an interpretative communication.

The Commission encourage all actors involved to endeavour to reduce national divergences

Different activities will be conducted for this purpose.

– *The Work Programme will continue*

The measures outlined in 2003 were appropriate then, and continue to be so now, for improving the implementation of the Directive.

The activities listed in the Work Programme will be continued, and the involvement of all stakeholders is a solid basis to strive for better implementation of the principles of the Directive.

– *The Working Party should improve its contribution to harmonising practice*

The Working Party, bringing together national data protection supervisory authorities, is a key element in ensuring better and more coherent implementation. Accordingly, this body has the task to "*examine any question covering the application of the national measures adopted under this Directive in order to contribute to the uniform application of such measures*". It has already conducted useful work in seeking uniform national application of key provisions, such as those on transborder data flows or on the concept of personal data.

In order to reap the full benefit of this mandate, Data Protection authorities should also strive to adapt their domestic practice to the common line they decide at the Working Party.

Taking up the challenges of new technologies

The principles contained in the Directive remain valid and should not be modified. However, the extensive development of new information and communication technologies necessitates specific guidance on how to apply those principles in practice. Increasingly sophisticated technology enables information to circulate rapidly around the world. However technology also enables better protection of data where required. Technology facilitates better control and searching of data. Relevant data can be identified more quickly and more easily. Where permission is not given to transmit data, technology enables this data to be isolated and protected more rapidly and effectively than before.

The Working Party has a very substantial role to play here. It should pursue the work carried out in its Internet Task Force and continue to develop a common approach among national data protection supervisory authorities to harmonize the implementation of national law, in particular as regards applicable law and transborder data flows.

Where a particular technology is found to consistently pose questions as regards the application of the data protection principles, and its widespread use or potential intrusiveness is considered to justify more stringent measures, the Commission could propose sector-specific legislation at EU level in order to apply those principles to the specific requirements of the technology in question. This approach was taken in Directive 2002/58/EC on privacy and electronic communications.

The ongoing review of this Directive, as well as the Communication on RFID mentioned above, may offer the opportunity to reflect on the need for modifying this Directive or for adopting specific rules to address data protection issues raised by technologies such as the Internet or RFID.

Providing a coherent response to the demand for public interest uses, especially for security

We need to reconcile two fundamental requirements: to effectively tackle threats to people's everyday life in Europe, especially in security matters, and at the same time to protect

fundamental rights, including data protection rights. There is an important amount of personal data collected on individuals and many activities where traces of personal data are left and stored. Data can only be used for different reasons to those for which it was originally collected when it is duly authorised. Such measures must be justified and necessary in a democratic society on public interest grounds, for example to fight terrorism and organised crime.

In striking the important balance between measures to ensure security and protect non-negotiable fundamental rights, the Commission makes sure that it protects personal data as guaranteed by Article 8 of the Charter of Fundamental Rights. The EU works with external partners also. This is essential in a globalised world. In particular the EU and USA have a continuous transatlantic dialogue to discuss information sharing and the protection of personal data for law enforcement purposes.

The Commission will consider the implementation of the Directive once again upon conclusion of the measures laid out in this Communication.