European Economic and Social Committee

SOC/402
Personal data protection

Brussels, 16 June 2011

OPINION

of the
European Economic and Social Committee
on the
Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions – A comprehensive approach on personal data protection in the European Union
COM(2010) 609 final

_____

Rapporteur: **Mr Morgan**

_____

Rue Belliard/Belliardstraat 99 — 1040 Bruxelles/Brussel — BELGIQUE/BELGIË
Tel. +32 25469011 — Fax +32 25134893 — Internet: http://www.eesc.europa.eu

On 4 November 2010 the European Commission decided to consult the European Economic and Social Committee, under Article 304 of the Treaty on the Functioning of the European Union, on the

> *Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions – A comprehensive approach on personal data protection in the European Union*
> COM(2010) 609 final.

The Section for Employment, Social Affairs and Citizenship, which was responsible for preparing the Committee's work on the subject, adopted its opinion on 27 May 2011.

At its 472nd plenary session, held on 15 and 16 June 2011 (meeting of 16 June 2011), the European Economic and Social Committee adopted the following opinion by 155 votes to 9 with 12 abstentions.

*

* *

1. Conclusions and recommendations

1.1 EU Data Protection Law is based on the 1995 Directive (95/46 EC). It had two objectives, expressed as follows:

(1) Member States shall protect the fundamental rights and freedoms of natural persons and in particular their right to privacy with respect to the processing of personal data.
(2) Member States shall neither restrict nor prohibit the free flow of personal data between Member States for reasons connected with the protection afforded under paragraph (1).

It is essential to achieve a balance between these objectives so that they are not in conflict. The main objective of new legislation must be to put in place a legal framework to help achieve both objectives.

1.2 The EESC welcomes this Communication which outlines the Commission's approach to updating the Data Protection Directive 95/46 EC. The explosive development of new technologies is causing an exponential increase in the amount of on-line data processing which requires a parallel increase in personal data protection if large scale intrusion into personal privacy is to be avoided. The collection, merging and management of data from multiple sources need to be carefully circumscribed. The public sector holds many different files on aspects of the relationship between citizens and the state. Data collected should be the minimum required for each purpose and there must be a ban on assembling these various data into a "big brother" data base.

1.3 At the same time, the EESC urges caution. Legislation regulating business activity must remain stable and predictable. The EESC therefore supports an appropriate revision of the Data Protection Directive.

1.4 The Communication recognises that a main recurrent concern of stakeholders, particularly multinational companies, is the lack of sufficient harmonisation between Member States' legislation on data protection, in spite of a common EU legal framework. The EESC proposes that the new legislation provide more consistent protection of workers' personal data throughout the EU including a European framework to strengthen legal clarity and certainty. In this respect the EESC welcomes in particular the intention to make the appointment of an independent Company Data Protection Officer mandatory and to harmonize the rules related to their tasks and competences.

1.5 Given the possible conflict between the privacy of the individual and the commercial exploitation of data about that individual and the high stakes involved, people need to become increasingly aware of the purposes for which their data is collected and the powers they have to control it when it has been collected. Therefore the EESC believes that effective enforcement and redress are a sine qua non if this project is to be truly 'comprehensive'. Furthermore, the cross border dimension must be covered.

1.6 As far as EU citizens are concerned, the relevant law within the European Union should be that of the Member State of the data controller, wherever the data is held. For people entitled to protection, especially employees and consumers, the data protection law of their usual place of residence should apply.

1.7 The reference to children is cursory. There needs to be a specific focus on child related privacy issues. The right to be forgotten could correct the record of childish foolishness and teenage misdemeanours but the right to be forgotten may not, in fact, be realisable.

1.8 The present definition of sensitive data needs to be clarified as the categories of electronic data about individuals continue to increase. The widespread and indiscriminate use of surveillance cameras is of concern to the EESC. It is essential to enforce the law restricting the misuse of these images. GPRS data relating to an individual's location is another contentious issue. The capture of biometric data is increasing. The definition should accommodate such new technologies and methodologies and it should allow for further technological developments. It may be necessary to establish principles related to contexts. The EESC is in favour of the appropriate use of these new technologies.

1.9 While acknowledging the sensitivities of inter-state police co-operation, the EESC believes that it is essential that fundamental rights, including personal data protection, receive maximum consideration at all times.

1.10 The EESC supports the Commission's general thrust to ensure a more consistent application of EU data protection rules across all Member States. The EESC is worried that all 12 NMS may not yet have completed full and effective implementation of Directive 95/46.

1.11 It is the opinion of the EESC that national data protection authorities are generally toothless and overworked and that their independence needs to be reinforced. Any new Directive should require that national authorities have the status, authority and resources to fulfil their role.

1.12 Based on its contribution so far to the protection of individuals with regard to the processing of personal data, the EESC believes that there is a valuable on-going role for the Article 29 Working Party.

1.13 In the context of the EU Digital Agenda, the EESC asks the Commission to consider the establishment of an EU Authority to consider the broader societal ramifications of the Internet on a 10 to 20 year timescale. Present provisions for personal data security and general cyber security are becoming increasingly inadequate. Society is playing catch-up. In the context of data protection, the EESC recommends the appointment of an EU-wide Data Protection Supervisor. The present EU Data Protection Supervisor is concerned only with EU Institutions. What is needed is a supervisor responsible for Member State co-ordination and operational standards. Such an appointment would, however, provide only one part of the overarching Authority envisaged by the Committee.

2. Introduction

2.1 The EESC continues to support the principles on which the 1995 Directive was based. The following are simplified and unqualified extracts from the text of the Directive. They clearly express the principles involved:

- Article 6

Member States shall provide that personal data must be:

(a) processed fairly and lawfully;
(b) collected for specified, explicit and legitimate purposes;
(c) adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed;
(d) accurate and, where necessary, kept up to date;
(e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the data were collected.

- Article 7

Member States shall provide that personal data may be processed only if:

(a) the data subject has unambiguously given his consent; or
(b) processing is necessary for the performance of a contract to which the data subject is party; or
(c) processing is necessary for compliance with a legal obligation to which the controller is subject; or
(d) processing is necessary in order to protect the vital interests of the data subject; or
(e) processing is necessary for the performance of a task carried out in the public interest; or
(f) processing is necessary for the purposes of the legitimate interests pursued by the controller).

- Article 8

Member States shall prohibit the processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and the processing of data concerning health or sex life.

2.2 In the last decade, circumstances have changed significantly with new provisions in Article 16 of the Treaty of Lisbon and Article 8 of the Charter of Fundamental Rights.

2.3 This Communication intends to lay down the Commission's approach for modernising the EU legal system for the protection of personal data in all areas of the Union's activities, taking account, in particular, of the challenges resulting from globalisation and new technologies, so as to continue to guarantee a high level of protection of individuals with regard to the processing of personal data in all areas of the Union's activities.

2.4 Nowadays the exchange of information across the globe has become easier and faster. An individual's personal data – email, photos and electronic agendas – may be created in the UK using software hosted in Germany; processed in India; stored in Poland and accessed in Spain by an Italian citizen. This rapid increase in information flows around the world presents a big challenge for individuals' rights to personal data privacy. Data protection issues, including their cross-border dimension, affect people every day – at work, in dealing with public authorities, when buying goods or services, or when travelling or surfing the internet.

2.5 In 2011 the Commission will propose legislation aimed at revising the legal framework for data protection with the objective of strengthening the EU's stance in protecting the personal data of the individual in the context of all EU policies, including law enforcement and crime prevention, taking into account the specificities of these areas. Non-legislative measures, such

as encouraging self-regulation and exploring the feasibility of EU privacy seals, will be pursued in parallel.

2.6 The Commission will also continue to ensure the proper monitoring of the correct implementation of Union law in this area, by pursuing an active infringement policy where EU rules on data protection are not correctly implemented and applied.

2.7 The comprehensive approach to data protection has the following key objectives:

- Strengthening individuals' rights;
- Enhancing the internal market dimension;
- Revising the data protection rules in the area of police and judicial co-operation in criminal matters;
- The global dimension of data protection;
- A stronger institutional arrangement for better enforcement of data protection rules.

Sections 3 to 7 below summarise these objectives and give the EESC perspective on the proposals. The headings in **Bold** follow the structure of the Communication. The text in *italics* is a synopsis of the text.

3. Strengthening Individuals' Rights

3.1 Ensuring appropriate protection for individuals in all circumstances

The Charter of Fundamental Rights includes the right to the protection of personal data. The definition of personal data aims at covering all informational relating to an identified or identifiable person. Consideration will be given to means to ensure a coherent application of data protection rules, taking into account the impact of new technologies on individuals' rights and freedoms and the objective of ensuring the circulation of personal data within the internal market.

3.1.1 The free circulation of personal data within the internal market is necessary for a fully functioning market; however, it does pose a threat to the privacy of data held by companies about employees. Specific safeguards are needed, such as the accountability of data controllers for multi-national data exchange and the use of encryption for more sensitive data.

3.1.2 The EESC would like to stress that the employment sector is more or less excluded from not only in the current Communication but also from the whole debate on data-protection in Europe. The work already done at European level should be used as a starting point, in particular the proposals put forward by the Article 29 Working Party.

3.2 Increasing transparency for data subjects

Transparency is a fundamental condition for enabling individuals to exercise control over their own data and to ensure effective protection of personal data. Consideration will be given to a general principle of transparent processing, specific obligations for data controllers, particularly in relation to children, standard privacy information notices and a mandatory personal breach notification.

3.2.1 Standard notices are preferable since they obviate conflicts of interest. Their use should be voluntary.

3.2.2 Transparency does not necessarily address the issue of one sided contract terms. It is important to develop stricter rules to provide greater protection against unfair terms.

3.2.3 The reference to children is cursory. There needs to be a specific focus on child related privacy issues. The right to be forgotten could correct the record of childish foolishness and teenage misdemeanours but the right to be forgotten may not, in fact, be realisable. (3.3.2 below).

3.2.4 The new legislation must clarify the role of the person responsible for processing data and the person responsible for recording data so that there is no confusion about their identities and the obligations and rights that each of them has.

3.2.5 The EESC supports the proposal for mandatory breach notification but believes that it may not be applicable to all events in all sectors in all circumstances.

3.3 Enhancing control over one's own data

Important preconditions are limitations to data processing in relation to its purpose (principle of data minimisation) and effective control by data subjects over their own data. Consideration will be given to strengthening the principle of data minimisation, improving the modalities for exercising rights of access, rectification, erasure or blocking of data, clarifying the right to be forgotten and ensuring the explicit right of data portability.

3.3.1 In general the EESC supports every move to enhance personal privacy. Individuals should have a right of free access to any data collected about them. Free access to credit rating data would be a case in point. The withdrawing of consent without reason and an effective right to be forgotten are fundamental, but privacy would be further enhanced if less data were collected in the first place. Hence the EESC urges the Commission to give real effect to the proposal to strengthen the principle of data minimisation.

3.3.2 While the right to be forgotten is an attractive concept, it will be difficult to achieve, given the viral nature of data on the internet and technologies which delete but do not forget.

3.4 Raising awareness

Awareness raising activities should be encouraged, including the provision of information on web sites, clearly spelling out data subjects' rights and data controllers' responsibilities. Young people's lack of awareness is a particular concern.

3.4.1 It will be difficult to achieve the necessary behavioural change, especially in view of the fact that rapid development of social networks has not been accompanied by an increase in awareness amongst users of the implications of the quantities of data which they provide. While, in principle, mandatory awareness notices on every internet service would be nice to have, they could be problematical for business. Consideration should be given so awareness protocols by category of service – internet commerce, ISPs, Search Engines, Social Networks, etc.

3.4.2 The EESC welcomes the intention of the Commission to offer EU funding to support awareness raising activities. The EESC would like this to be extended to the co-funding of awareness raising activities by Social Partners and Civil Society Organisations at European and national level.

3.5 Ensuring informed and free consent

The Commission will examine ways of clarifying and strengthening the rules of consent.

3.5.1 The types of consent required should continue be linked to the type of data being processed and not the type of technology used. However, the EESC is concerned that in most cases, when consent is given in an internet environment, the application does not provide any confirmation of that agreement, nor are there effective mechanisms to record the withdrawal of consent. In addition, agreement may involve clicking a button to agree to reams of terms and conditions, of which consent may be a small element. It would make sense for consent relative to data control to be a simple and separate document so that it could be meaningful, informed and specific.

3.5.2 For organisations and businesses which carry out their activities on the Internet, the processing of personal information is vital. The default option is clearly advantageous to the operator but, if not fairly implemented, it may disadvantage the client. Its use should be circumscribed so that all operators are bound to offer privacy by default to their clients if the clients so wish.

3.5.3 For consent to be freely given, the contract must also be fair. Principles need to be established to avoid unfair commercial practices.

3.6 Protecting sensitive data

Consideration will be given to expanding the definition of 'sensitive data' to include, for example, genetic data and the further harmonisation of the conditions for processing sensitive data.

3.6.1 The present definition of sensitive data needs to be clarified as the categories of electronic data about individuals continue to increase. The widespread and indiscriminate use of surveillance cameras is of concern to the EESC. It is essential to enforce the law restricting the misuse of these images. GPRS data relating to an individual's location is another contentious issue. The capture of biometric data is increasing. The definition should accommodate such new technologies and methodologies and it should allow for further technological developments. It may be necessary to establish principles related to contexts. The EESC is in favour of the appropriate use of these new technologies.

3.6.2 Enhanced protection for sensitive data should also be provided. Encryption should be mandatory for certain sensitive data. The best available technologies should be applied. Controllers should be accountable for security breaches.

3.7 Making remedies and sanctions more effective

Consideration will be given to extending the powers to bring actions before national courts and the possible inclusion of criminal sanctions for serious violations.

3.7.1 Given the possible conflict between the privacy of the individual and the commercial exploitation of data about that individual and the high stakes involved, people need to become increasingly aware of the purposes for which their data is collected and the powers they have to control it when it has been collected. Therefore the EESC believes that effective enforcement and redress are a sine qua non if this project is to be truly "comprehensive". Furthermore, the cross border dimension must be covered.

3.7.2 The case for collective redress should be examined as a remedy for extreme protection failures. Consideration should be given to the case for business and professional organizations and trade unions to represent individuals and bring an action before courts.

4. **Enhancing the Internal Market Dimension**

4.1 Increasing legal certainty and providing a level playing field for data controllers

Data protection in the EU has a strong internal market dimension. Consideration will be given to the means to achieve further harmonisation of data protection rules at EU level.

4.1.1 The EESC is concerned that the scope of Member State decision making provided by the text of Directive 95/46 has created an implementation problem. A Regulation in this context might have provided more certainty. Harmonisation should be implemented around a body of standards sufficient to satisfy the requirements of the Directive.

4.1.2 Throughout the Communication, there is no reference to employees and the access to their personal data which is held by employers. In multinational firms which may centralise records within or even outside the EU, employees need clearly defined rights of access to be part of the new legislation.

4.2 Reducing the administrative burden for controllers

Different possibilities will be explored for the simplification and harmonisation of the current notification system, including the possible drawing up of a uniform EU-wide registration form. Notifications could be published on the internet.

4.2.1 The EESC would very much support these initiatives.

4.3 Clarifying the rules on applicable law and Member States' responsibility

It is not always clear to data controllers and data protection supervisory authorities which Member State is responsible and which law is applicable when several Member States are involved. Globalisation and technological developments are making this problem worse. Revision and clarification of the existing provisions on applicable law will be examined in order to improve legal certainty and clarify Member State responsibilities.

4.3.1 As far as EU citizens are concerned, the relevant law within the European Union should be that of the Member State of the data controller, wherever the data is held. For people entitled to protection, in particular employees and consumers in the EU, the provisions and procedures of data protection law of their usual place of residence should apply.

4.4 Enhancing data controllers' responsibility

The Commission will explore ways of ensuring that data controllers put in place effective policies and mechanisms to ensure compliance with data protection rules. Consideration will be given to making the appointment of a data protection officer mandatory and harmonising their rules of engagement, to create an obligation for data protection impact assessment. In addition, the Commission will further promote the use of Privacy Enhancing Technologies (PETs) and the implementation of the concept of 'Privacy by Design'.

4.4.1 PETs and Privacy by Design have the potential to remove discretion from data controllers, who may otherwise be conflicted by the commercial priorities of their organisations. The EESC urges the Commission to initiate further study and development of these tools since

they have the potential to enhance data protection while removing conflicts of interest. Ideally, these tools could become mandatory.

4.4.2 For the avoidance of doubt, data controllers should be accountable for all aspects of the processing of data for which they are responsible. Accordingly, where sub-contractors and or operations in other countries are involved, the personal privacy obligations should be fully spelled out in the contract.

4.4.3 The EESC believes that each Member State should establish a professional body to be responsible for the skills and certification of DPOs.

4.4.4 Implementation of provisions under this heading should be consistent with the goal of reducing the administrative burden of data controllers covered in point 4.2.

4.5 Encouraging self-regulatory initiatives and exploring EU certification schemes

The Commission will examine means to further encourage self-regulatory initiatives such as codes of conduct and explore the feasibility of EU certification schemes.

4.5.1 See 3.7.1 above: enforcement and redress are key concerns of the EESC. These proposals are attractive in as much as they may help to reduce the enormous burden of regulation born by business. A compendium or guide to best practice should be sponsored in each Member State.

5. Revising the Data Protection Rules in the area of police and judicial co-operation in criminal matters

The EU instrument for the protection of personal data in the areas of police and judicial co-operation in criminal matters is a 2008 JHA Framework Decision. It has many shortcomings which may affect the possibilities for individuals to exercise their data protection rights in such areas as knowing what personal data are being processed and exchanged about them, by whom and for what purpose, and how to exercise their rights such as the right to access their data.

Consideration will be given to the extension of the application of general data protection rules to the areas of police and judicial co-operation in criminal matters, to the introduction of new provisions in domains such as the processing of genetic data, launching a consultation on the revision of supervision systems in this area and assessing the need for the long term alignment of various sector specific rules within the new general legal data protection framework.

5.1 While acknowledging the sensitivities of inter-state police co-operation, the EESC believes that it is essential that fundamental rights, including personal data protection, receive maximum consideration at all times. The EESC is afraid that security concerns, however

spurious, are frequently causing fundamental rights to be over ridden. Individuals need to be better informed about the methods and purposes by and for which the authorities collect personal data from telephone billing, bank accounts, airport controls, etc.

6. The global dimension of data protection

6.1 Clarifying and simplifying the rules for International data transfer

The Commission intends to examine how to

- *improve and streamline current procedures for international data transfers to ensure a more uniform and coherent EU approach vis-à-vis third countries and international organisations,*
- *better specify the criteria and requirements for assessing the level of data protection in a third country or international organisations,*
- *define core EU data protection elements for use in international agreements.*

6.1.1 The EESC supports these worthwhile initiatives and hopes that the Commission can achieve the broad international agreement without which these proposals may be less than effective.

6.2 Promoting universal principles

The European Union must remain a driving force behind the development and promotion of international legal and technical standards for the protection of personal data. To this end the Commission will be active in the international standards arena and in co-operation with third countries and international organisations such as the OECD.

6.2.1 Again, the EESC is supportive. Given the global nature of the Internet it is essential that rules and guidelines are compatible between continents. Personal data must have cross border protection. We note that OECD guidelines already exist, as does the Council of Europe Convention 108. This latter Convention is in the process of being revised. The Commission should ensure that the Convention and the new Directive are compatible.

7. A stronger institutional arrangement for better enforcement of data protection rules

The Commission will examine:

- *how to strengthen, clarify and harmonise the status and the powers of the national data protection authorities;*
- *ways to improve the co-operation and co-ordination between data protection authorities;*
- *how to ensure a more consistent application of EU data protection rules across the internal market. Measures could include:*
  - *strengthening the role of national data protection supervisors;*

- *better co-ordinating their work via the Article 29 working party;*
- *creating a mechanism to ensure consistency under the authority of the European Commission.*

7.1 Given the EESC concerns about enforcement and redress, these proposals are key issues for the Committee. We endorse the phrases 'strengthen, clarify and harmonise' and 'co-operation and co-ordination' and we support the Commission's general thrust to ensure a more consistent application of EU data protection rules across all Member States. The EESC is worried that all 12 NMS may not yet have completed full and effective implementation of Directive 95/46.

7.2 It is the opinion of the EESC that national data protection authorities are generally toothless and overworked and that their independence needs to be reinforced. Any new Directive should require that national authorities have the status, authority and resources to fulfil their role. Their tasks and resources should be defined on a pan-EU basis. Consideration should be given to the appointment of an EU Data Protection Supervisor.

7.3 Based on its contribution so far to the protection of individuals with regard to the processing of personal data, the EESC believes that there is a valuable on-going role for the Article 29 Working Party.

Brussels, 16 June 2011.

The President
of the
European Economic and Social Committee

Staffan Nilsson

*

* *

N.B.: Appendix overleaf

Appendix
to the opinion
of the European Economic and Social Committee

The following section opinion text was rejected in favour of amendments adopted by the assembly, although at least one-quarter of the votes cast were in favour of retention of the section opinion text:

Point 1.6

As far as EU citizens and EU employees are concerned, the relevant law within the European Union should be that of the Member State of the data controller, wherever the data is held.

Point 4.3.1

As far as EU citizens and EU employees are concerned, the relevant law within the European Union should be that of the Member State of the data controller, wherever the data is held.

Outcome

86 votes for amending these paragraphs,
72 against,
19 abstentions.