

# EUROPEAN PARLIAMENT

1999



2004

---

*Session document*

FINAL  
A5- 0177/2000

22 June 2000

## REPORT

on the Draft Commission Decision on the adequacy of the protection provided by the Safe Harbour Privacy Principles (C5-0280/2000 – 2000/2144(COS))

Committee on Citizens' Freedoms and Rights, Justice and Home Affairs

Rapporteur: Elena Ornella Paciotti



## CONTENTS

	<b>Page</b>
PROCEDURAL PAGE .....	4
MOTION FOR A RESOLUTION .....	5

## PROCEDURAL PAGE

By letter of 6 June 2000, the Commission forwarded to Parliament her Draft Decision on the adequacy of the protection provided by the Safe Harbour Privacy Principles 2000/2144(COS)).

At the sitting of 13 June 2000 the President of Parliament announced that she had referred this Draft Decision to the Committee on Citizens' Freedoms and Rights, Justice and Home Affairs as the committee responsible (C5-0280/00).

The Committee on Citizens' Freedoms and Rights, Justice and Home Affairs had appointed Elena Ornella Paciotti rapporteur at its meeting of 11 April 2000..

It considered the Draft Commission Decision and the draft report at its meetings of 5 June and 21 June 2000.

At the last meeting it adopted the motion for a resolution by 21 votes to 0 , with 16 abstentions.

The following were present for the vote: Graham R. Watson, chairman, Robert J.E. Evans, vice-chairman, Elena Ornella Paciotti, rapporteur, Jan Andersson (for Anna Karamanou), Mary Elizabeth Banotti, Maria Berger (for Margot Keßler), Christian von Boetticher, Alima Boumediene-Thiery, Marco Cappato, Michael Cashman, Carmen Cerdeira Morterero (for Gerhard Schmid), Ozan Ceyhun, Carlos Coelho, Gérard M.J. Deprez, Giuseppe Di Lello Finuoli, Olivier Duhamel, Carlo Fatuzzo (for Rocco Buttiglione, pursuant to rule 153(2)), Francesco Fiori (for Marcello Dell'Utri, pursuant to rule 153(2)), Robert Goodwill (for Daniel J. Hannan, pursuant to rule 153(2)), Christopher Heaton-Harris (for Timothy Kirkhope, pursuant to rule 153(2)), Ewa Klamt, Alain Krivine (for Pernille Frahm), Klaus-Heiner Lehne (for Charlotte Cederschiöld), Baroness Sarah Ludford, Minerva Melpomeni Malliori (for Joke Swiebel), Lucio Manisco (for Fodé Sylla), Francesco Musotto (for Thierry Cornillet), Hartmut Nassauer, Ana Palacio Vallelersundi (for Jorge Salvador Hernández Mollar), Hubert Pirker, Martin Schulz, Sérgio Sousa Pinto, Anna Terrón i Cusí, Alexandre Varaut (for Mogens N.J. Camre), Gianni Vattimo, Dominique Vlasto (for Bernd Posselt), Jan-Kees Wiebenga.

The explanatory statement will be presented orally in plenary sitting.

The report was tabled on 22 June 2000.

The deadline for tabling amendments will be indicated in the draft agenda for the relevant part-session .

## MOTION FOR A RESOLUTION

### **European Parliament resolution on the Draft Commission Decision on the adequacy of the protection provided by the Safe Harbour Privacy Principles (C5-0280/2000 – 2000/2144(COS))**

*The European Parliament,*

- having regard to Directive 95/46/EC, particularly Article 25 thereof,
- having regard to the draft Commission Decision on the adequacy of the protection provided by the Safe Harbour Privacy Principles (C5-0280/2000),
- having regard to the opinion (WP 32) on this subject adopted unanimously on 16 May 2000 by the working party of national representatives provided for under Article 29 of Directive 95/46/EC, the opinions delivered previously on the same question (WP12 and WP27),
- having regard to the opinion of 31 May 2000 delivered by the Committee provided for in Article 31 of the same Directive,
- having regard to Article 8 and the relevant implementing rules of the Council decision of 28 June 1999 (1999/468/EC)<sup>1</sup>,
- having regard to Rule 88 of its Rules of Procedure,
- having regard to the report by the Committee on Citizens' Freedoms and Rights, Justice and Home Affairs (A5-0177/2000),

*in general, as regards the meaning of data protection in the framework of the competences of the Union*

A. whereas

- (a) the development of the information society and electronic commerce have led at global level to an exponential increase in the movement of data and the risks involved in the misuse of such data;
- (b) such abuses not only act as a brake on the development of e-commerce in that they undermine the confidence of consumers, but also often constitute an infringement of the rights and freedoms of persons and, in particular, an invasion of privacy;
- (c) protecting data means protecting the people to whom the information being processed

---

<sup>1</sup> OJ L 184, 17.7.1999, p. 23

relates, and such protection is one of the fundamental rights recognised by the Union (Article 8 of the European Convention for the Protection of Human Rights, referred to in Article 6 of the Treaty on European Union and Article 286 of the EC Treaty);

- (d) Directive 95/46/EC, which is modelled on Council of Europe Convention N°108 (1981) and the OECD (1980) and the UN guidelines (1990), is based on identifying rights for the data subject and corresponding obligations on those who process data or who exercise control over such processing;
- (e) such protection would be useless if it were confined to the territory of the Union and did not also provide adequate protection, as provided for by the directive, in the third countries to which the data is transferred;
- (f) an adequate level of protection for personal data in all the countries to which data can be transferred is also required, in order to avoid a situation where different levels of protection allow distortions in the use of data and relocation of its treatment in violation of the GATS agreements;
- (g) the Commission must ensure, on behalf of the citizens of the Union and its Member States, that 'adequate' protection exists in the third countries;

*in general, as regards the role of the Commission and the measures and criteria that it must adopt in order to evaluate the 'adequacy' of the protection provided by third countries*

B. whereas:

- (a) in evaluating the 'adequacy' of the protection provided by third countries, the Commission must take account of the varying levels of legal, economic and technological development of the third countries in relation to European standards;
- (b) 'adequate' protection does not mean per se that the third country should have the same rules as the Union but that, regardless of the type of legislative protection in force in the third country, the owner of the data must be effectively protected;
- (c) in a third country protection should be considered effective when its effectiveness can be measured with reference to objective data, such as the possibility of identifying the type of data processed, the uses that may be made of it and the mechanisms created to guarantee protection;
- (d) in this context, the protection provided by a third country must comply with the following minimum requirements set out by the data control authorities of the EU Member States (opinion WP12 of June 1998):

"(1) **the purpose limitation principle** - data should be processed for a specific purpose and subsequently used or further communicated only insofar as this is not incompatible with the purpose of the transfer. The only exemptions allowed should be those necessary in a democratic society on one of the grounds listed in Article 13 of the directive.

- (2) **the data quality and proportionality principle** - data should be accurate and, where necessary, kept up to date. The data should be adequate, relevant and not excessive in relation to the purposes for which they are transferred or further processed.
- (3) **the transparency principle** - individuals should be provided with information as to the purpose of the processing and the identity of the data controller in the third country, and other information insofar as this is necessary to ensure fairness. The only exemptions permitted should be in line with Articles 11(2) note 3 and 13 of the directive.
- (4) **the security principle** - technical and organisational security measures should be taken by the data controller that are appropriate to the risks presented by the processing. Any person acting under the authority of the data controller, including a processor, must not process data except on instructions from the controller.
- (5) **the rights of access, rectification and opposition** - the data subject should have a right to obtain a copy of all data relating to him/her that are processed, and a right to rectification of those data where they are shown to be inaccurate. In certain situations he/she should also be able to object to the processing of the data relating to him/her. The only exemptions to these rights should be in line with Article 13 of the directive.
- (6) **restrictions on onward transfers** - further transfers of the personal data by the recipient of the original data transfer should be permitted only where the second recipient (i.e. the recipient of the onward transfer) is also subject to rules affording an adequate level of protection. The only exceptions permitted should be in line with Article 26(1) of the directive".
- (7) With reference to the guarantees concerning the effective implementation it is also necessary to secure the following objectives, particularly if the rules relating to the processing of data subject to assessment are based on a system of self-regulation:
  - The instrument must have mechanisms which effectively ensure a good level of general compliance. A system of dissuasive and punitive sanctions is one way of achieving this. Mandatory external audits are another.
  - The instrument must provide support and help to individual data subjects who are faced with a problem involving the processing of their personal data. An easily accessible, impartial and independent body to hear complaints from data subjects and adjudicate on breaches of the code must therefore be in place.
  - The instrument must guarantee appropriate redress in cases of non-compliance. A data subject must be able to obtain a remedy for his/her problem and compensation as appropriate.

with specific reference to the data protection system used in the United States

C. whereas in the United States:

- (a) there is not at present any generally applicable legal data protection in the private sector and virtually all data are currently processed without specific guarantees of judicial protection;
- (b) there are, however, numerous legislative proposals pending before Congress and the President of the United States himself recently referred to the need for further legislative measures, while the Federal Trade Commission expressed the same opinion in its third report to Congress on the functioning of the system of self-regulation in the electronic marketplace ;
- (c) the guidelines approved by the OECD must in any case be applied in the area of personal data protection (signed by the USA in 1980 and ratified at the Ottawa OECD Conference in September 1998);

with specific reference to the nature and scope of the enforceability of the safe harbour

- D. whereas, rather than encouraging a legislative approach, the Department of Commerce intends to propose to companies 'safe harbour privacy principles' (and the Frequently Asked Questions arising from such principles), which:
- (a) will apply only to personal data of EU origin, with the status of the voluntary 'standard' suggested to the businesses intending to receive data from the EU, but are binding on those businesses that opt to adhere to them and are enforceable by private dispute resolution bodies and government bodies with powers to obtain relief against unfair or deceptive practices;
  - (b) relate only to firms which fall within the competence of the Federal Trade Commission and the Department of Transportation (so that, for example, firms in the banking and telecommunications sectors are excluded);
  - (c) are subject to exceptions (FAQ 15 ) as regards public record and publicly available data (e.g. land register, telephones, tax declarations, electoral rolls), which are protected by Community legislation;
  - (d) use ambiguous terms such as 'organisation' (which may refer both to businesses and business conglomerates) and 'explicit authorisations' (which allow exemptions to the principles);
  - (e) do not provide a right of effective, personal appeal to a public body (FAQ 11);
  - (f) do not allow it to be concluded with certainty that it will be possible to obtain compensation for individual damage suffered as a result of possible violations of the safe harbour principles;



1. As a preliminary matter, and irrespective of the question of the draft decision submitted to Parliament:
  - (a) Notes with concern that, almost two years after the directive's entry into force, data relating to EU citizens are circulating in third countries without any effective control by the Commission or the Member States;
  - (b) Wonders to what extent data relating to EU citizens may have been misused already;
  - (c) Requests the Member States and the Commission to inform EU citizens of the risks attached to the circulation of data in countries where data protection is not ensured or the Commission has not yet completed the process of assessing the adequacy of any such protection;
  - (d) Considers that the Commission was responsible for a serious omission in failing to draw up, before the directive's entry into force, standard contractual clauses that EU citizens could invoke in the courts of third countries;
  - (e) Establishes 30 September as the date by which the proposed standard clauses should be submitted to the Committee set up under Article 31 of the directive;
  - (f) Reserves the right, in the event of failure to comply, to launch the procedures provided for in the Treaty in respect of failure to act;

*Concerning the draft decision submitted to European parliament*

2. Points out that the draft decision does not describe a situation currently in existence in the United States, but is based on a draft of the safe harbour principles (with the relevant explanations) which the United States Department of Commerce will issue for the guidance of companies wishing to meet the adequate protection requirement of Directive 95/46/EC;
3. Draws the Commission's attention to the risk that the exchange of letters between the Community authorities and the US Department of Commerce on the implementation of the 'safe harbour' principles could be interpreted by the European and/or American judicial authorities as having the substance of an international agreement adopted in breach of Article 300 of the TEC and the requirement to seek Parliament's assent. (Judgement of the Court of Justice of 9 August 1994. French Republic v. the Commission - Commission/US agreement. Case C-327/91);
4. Regrets that, in the course of the last two years, there has been no consultation of European undertakings with regard to the risk of discrimination in relation to US undertakings which would be subject to less onerous data protection requirements than those with which European undertakings must comply;

5. Regrets that, in contrast with the US authorities' consultation of NGOs active in the field of consumer protection, the Commission has not embarked on any such consultation of European NGOs;
6. Calls into question the existence in the US of two different protection systems depending on whether or not the owners of the data are European, and wonders whether such a dual system complies with the clause prohibiting discrimination on the grounds of nationality contained in the relevant international (OECD) agreements;
7. Takes the view that, if issued and implemented by individual firms, such principles and the relevant explanations could be considered adequate protection under the terms of Article 25 of Directive 95/46/EC provided that the following changes are made to them:
  - recognition of an individual right of appeal to an independent public body instructed to consider any appeal relating to an alleged violation of the principles;
  - the obligation for participating firms to compensate for the damage, whether moral or to property, suffered by those involved, in the event of violations of the principles, and the undertaking by the firms to cancel personal data obtained or processed in an unlawful manner;
  - ease of identification of the steps to be taken to ensure data are cancelled and to obtain compensation for any damage suffered;
  - provision of a preliminary check by the Commission on the proper functioning of the system within six months of its entry into force and presentation of a report on the outcome of the check and any problems encountered to the Working Group referred to in Article 29 and the Committee referred to in Article 31 of the Directive, as well as to the relevant committee of the European Parliament;
8. Takes the view that the adequacy of the system cannot be confirmed and, consequently, the free movement of data cannot be authorised until all the components of the safe harbour system are operational and the United States authorities have informed the Commission that these conditions have been fulfilled;
9. Calls on the Commission to ensure that the operation of the safe harbour system is closely monitored, especially but not only as regards the points raised in paragraph 7 above and to make periodic reports to the working party provided for in Article 29 and the Committee provided for in Article 31 of Directive 95/46/EC, as well as to the relevant committee of the European Parliament;
10. Calls on the Commission and the Member States:
  - to provide appropriate information (in the Official Journal and via the Internet) for European citizens on the 'safe harbour', making clear that differences may continue to exist between the 'safe harbour' and European law as regards the processing of personal data;

- to set up help-lines (numero verde, guichet) to the relevant national authorities and the Commission to deal with any practical difficulties encountered (e.g. translations of appeals, forms, etc.);
  - to review the decision in good time in the light of experience and of any legislative developments;
11. Instructs its President to forward this resolution to the Commission and the Parliaments and Governments of the Member States.