EUROPEAN COMMUNITIES
THE COUNCIL

Brussels, 20 January 1992

10503/91
RESTREINT
ECO 208

OUTCOME OF PROCEEDINGS

of : Working Party on Economic Questions (Data Protection)
on : 12 and 13 December 1991

No. prev. doc.: 9754/91 ECO 184
No. Cion prop.: 8460/90 ECO 158 COM(90) 314 final - SYN 287

Subject: Protection of individuals in relation to the processing of personal data in the Community and information security


A. Additional principles to those contained in the Council of Europe Convention

2. Addressing the question as to whether additional principles to those contained in the Council of Europe Convention should be included in the Directive, note was taken of the following interventions:

3. The German delegation indicated that although the Council of Europe Convention was a good basis for the work of the Working Party, more detailed rules would have to be included in the Directive. In doing so the Working Party would have to examine in which way data was protected in the different Member States as the rules in this respect varied considerably. In
Germany, for example, there were very strict rules which could be considered as a ban against data processing with certain exceptions, whereas other countries had chosen a different approach. In deciding on what should be permissible an evaluation would have to be made between the interests of the users of the data and the data subjects.

In the German delegation's view the Working Party would also have to look at the question of controlling the use of data, an area in which the Council of Europe Convention had not given any guidance. Furthermore, the Working Party would have to examine the question of liability and the question of transfer of data to third countries.

4. The United Kingdom delegation indicated that the Directive would have to incorporate the principles of the Council of Europe Convention and contain clear rules on the liability of the data user and the role of the supervisory authorities. When discussing whether one should go beyond these principles it would, in the United Kingdom delegation's view, have to be borne in mind that the purpose of a Directive was to emphasize the ends but not the detailed means by which to achieve them. To agree in detail in, for example, Chapters II and III on how the principles of Article 16 should be implemented would not only be very difficult but did not seem necessary. What could be necessary would be to include certain clarifying provisions in the directive.

5. The French delegation agreed with the German delegation that it would be necessary to go beyond the rules of the Council of Europe Convention. To fulfill its purpose, the Directive should, in the French delegation's view, contain detailed rules leading to a high degree of harmonization in the Member States. In this context the French delegation mentioned the need for having rules as those set out in Chapter IV of the draft Directive which constituted an important addition to the Council of Europe Convention. Rules as those contained in Chapters II and III, reformulated on the lines suggested by the
French delegation in Working Document No 12, would also be necessary. In explaining its position, the French delegation stressed that it was important when data were to be sent to another state that the data subject had the same rights in that state. This implied that it would be necessary to go beyond Article 16 and the setting up of a minimum of procedural rules.

6. The Danish delegation indicated that additional rules in respect of, for example, an independent control authority and transfer of data to third countries would be necessary in the Directive. Comparing the structure of the Directive to a three step rocket where the first step would be the principles contained in Article 16 of the Directive, the second step the rules in Chapter IV and the last step the rules contained in Chapters II and III, the Danish delegation expressed doubts as to whether there would be a need for the last step.

7. Also the Greek and Portuguese delegations indicated that it would be necessary to go beyond the rules of the Convention.

8. Application of the principles contained in Article 16 of the draft Directive

8. Addressing the specific question as to whether the principles contained in Article 16 needed to be defined or supplemented in order to ensure a sufficient degree of harmonization in the Member States, the Chairman of the Working Party indicated that it might be necessary not only to supplement in, for example, Article 16(1)a the principles of fair collection with other principles but also to lay down basic conditions for lawful processing. In this context the Chairman of the Working Party suggested stipulating that processing of personal data only be considered lawful:

- with the explicit consent of the data subject, or

- where necessary for the execution of a contract with the data subject, or
- where necessary for the fulfillment of a legal obligation, or
- where necessary for the execution of a public function or duty, or
- where necessary to safeguard the legitimate interest of the controller, on condition that the interest of the data subject did not prevail.

9. In the Chairman's view the same grounds as proposed for lawful processing could also apply to lawful communication with possible additional grounds as for example those proposed by the Netherlands delegation of obtaining a right balance between the interests of third parties and the data subjects.

10. Reacting to the suggestions by the Chairman of the Working Party, the Danish delegation indicated that the application or implementation of the five criteria would be facilitated if a distinction was made between sensitive and non-sensitive data.

C. Level of protection agreed upon in the Directive

11. Taking as a starting point that Member States who so wished could go beyond the level of protection set by the Directive, the Working Party discussed if also in this area the Directive should set out certain rules to ensure a free flow of data between the Member States. In this context the Chairman of the Working Party suggested that the rules of reason originating from the "Cassis de Dijon" case could be taken as parameters when rules stricter than the common rules of the Directive were established in a Member State.

12. In the German delegation's view one possibility would be to agree on a subsidiary clause allowing Member States to set a higher level of protection than that provided by the Directive as long as this did not impede on the free flow of data.
Another possibility would, in the German delegation's view, be to set out a list with the areas (for example medical data), in which Member States could set stricter rules.

13. The Danish delegation indicated that one possible answer to the question of setting stricter rules lay in Article 6(2) of the draft directive which specified that Member States could set out the conditions under which the communication of personal data was lawful. By virtue of this provision a Member State who for example considered medical data as sensitive data could decide not to communicate this data to a third state on the condition that the principles laid down in the "Cassis de Dijon" ruling were respected.

14. The French delegation indicated that the only way of ensuring the free flow of data between the Member States would be to have a high level of harmonization by virtue of which the question of ensuring a free flow would become less important.

D. Discussion of Working Document No 12 from the French delegation

15. Following the invitation of the Chairman of the Working Party made at the Working Party's last meeting to reflect further on the suggestion by the French delegation contained in Working Document No 12, the Working Party resumed its discussions of this Working Document.

16. The Netherlands delegation indicated that it found the French delegation's suggestion of having a differentiated treatment depending on the nature of the data with the possibility in standard cases of not requiring a notification as attractive. The Netherlands delegation also agreed with the approach that certain data needed a more specific treatment. As regards, however, the proposal of prior authorization, the Netherlands delegation was of the opinion that alternative possibilities should be provided for.
17. The German delegation indicated that the suggestion by the French delegation gave rise to problems for this delegation. Bearing in mind the existing rules in Germany the French delegation’s suggestions were, in their present form, unacceptable. The German delegation, although agreeing that for example sensitive data be given particular consideration, did not think that each Member State should introduce a compulsory authorization system in this area. The supervisory authority should be given the possibility of examining the different cases but should not, in the German delegation’s view, have an obligation to do so.

18. The Irish delegation welcomed the move away from a distinction between the public and private sectors contained in the French delegation’s suggestions as well as the distinction made between different kinds of data. In the Irish delegation’s view the notification system contained in the French delegation’s document would, however, not only be cumbersome but unnecessary. The aim of transparency sought by a notification system could in the Irish delegation’s view be achieved by other means.

19. The Danish delegation recalled that at the last meeting of the Working Party it had received the French delegation’s suggestions with sympathy. It still welcomed the suggestions made by the French delegation but stressed that it would be necessary, although not in two separate chapters, to maintain a certain distinction between the private and public sectors.

20. Commenting on the first category suggested by the French delegation, the United Kingdom delegation indicated that the notification system was not the only means of obtaining transparency and that another possibility would be to provide that the data user made the contents of the file known on request. As regards the second category, the mechanism suggested by the French delegation that the supervisory authority give its opinion, could in the United Kingdom delegation’s view prove to be a very large and cumbersome task.
A better approach would be to empower the supervisory authority to give general guidance on what could or could not be done. Commenting on the suggestions by the French delegation in respect of the third category the United Kingdom delegation first of all indicated that it had a general problem concerning sensitive data as defined in the Directive which, in this delegation's view was a very wide definition. In the United Kingdom delegation's view the use of the concept "sensitive purposes" could narrow down the number of cases with potential problems. As regards more particularly the mechanism proposed by the French delegation in respect of sensitive data, the task foreseen for the supervisory authority went far beyond those foreseen in the United Kingdom. It was doubtful whether prohibition to handle certain data could be taken by an administrative decision and not a parliamentary decision. The mechanism suggested by the French delegation would furthermore entail that the processing could not start before the authorization had been given. The United Kingdom saw as an alternative to the approach suggested by the French delegation a notification to supervisory authority with the possibility of starting processing if the supervisory authority had not reacted within a specific time.

E. Discussion paper on Chapters II and III

21. Following the discussions of the Working Party, the Chairman of the Working Party drew up a document setting out a number of conclusions which could be drawn from the interventions by delegation made at the last as well as the present meeting. This discussion paper is set out in the Annex.

22. Reacting to the discussion paper drawn up by the Chairman, it was noted that a large majority of delegations as an initial reaction and pending further examination, agreed with the main lines set out in the discussion paper.
23. The United Kingdom delegation also welcomed the discussion paper but questioned the approach setting out criteria for processing to be lawful, thus considering processing as unlawful unless certain conditions were fulfilled. The United Kingdom delegation favoured the opposite approach, taking as a starting point that processing was lawful.

Commenting on the individual criteria for lawful processing set out in the discussion paper the United Kingdom delegation indicated that:

- as far as the requirement of the consent of the data subject was concerned it preferred the approach by which there was an assumption for processing unless objections were made;

- the requirement that the processing should be necessary for the execution of a contract would cover everyday commercial contracts and suggested to use the words "commercial relationships";

- the requirement that the processing should be necessary for the execution of a public function or duty should also cover public functions carried out by the private sector;

- the last criteria would create difficulties when having to be applied by the courts.

The United Kingdom delegation finally indicated that exceptions would have to be made for data already in the public domain.

24. The Luxembourg delegation, agreeing with the main lines of the discussion paper, indicated that the fourth criteria for lawful processing should make a reference to the purpose of the processing and agreed with the United Kingdom delegation that exemptions would have to be made for data already in the public domain.
25. The French delegation, referring to the second paragraph on page 2 of the discussion paper, stressed that the contents of this paragraph were only elements of reflection on which there was still no agreement.

F. Powers of the supervisory authorities

26. Discussing the powers of the supervisory authorities in the Member States, note was taken of the following interventions:

27. The Irish delegation explained that in Ireland the supervisory authority was independent and had wide powers. It could investigate possible infringements of any of the Council of Europe Convention principles, on complaints or ex officio and could enter the premises in which data were kept in order to examine them. If it decided that there had been a contravention it could issue an enforcement notice asking controllers to rectify, supplement or erase data. Failure to comply with an enforcement notice was considered an offence. The supervisory authority could also issue information notices asking for information necessary for the performance of its duties.

The supervisory authority could prohibit transborder flow of data if any of the principles in the Council of Europe Convention were not complied with and also played a role in registration of sensitive data.

Finally, the supervisory authority could draw up codes of conduct for certain business sectors.

28. Explaining the powers of the supervisory authority in France, the French delegation drew the attention of the Working Party to Articles 6, 8, 14, 15, 16, 21, 22, 23 and 31 of the French data protection law.
30. **The Spanish delegation** explained that the supervisory body foreseen in the Spanish bill would be independent of any ministry and would have its own work plan.

Notification to the supervisory authority would be obligatory. No processing could take place before the supervisory authority had given its authorization. In cases of serious infringement of citizens' rights by the data controller, the files could be frozen.

31. **The Greek delegation** explained that the Greek bill on data protection foresees the creation of an independent commission composed of persons nominated by the Supreme Court sitting in plenary session. The commission would issue guidelines concerning the application of the law and issue recommendations to the controller of the files and indicate to the competent authorities the cases where the law had not been abided by. It would draw up a report to be submitted by the Prime Minister and President of Parliament. In Greece processing of strictly personal data was forbidden unless a special law stipulated certain conditions. Processing of confidential data was allowed on the condition that there was not a special law prohibiting the processing and that there was an authorization or consent from the parties concerned and the processing was absolutely necessary. This rule on confidential data did, however, have certain exceptions. Processing of simple data was allowed if processed for special purposes and was not against the law.

32. **The German delegation** explained that in the public sector there was a notification system whereas this was with certain exemptions not the case in the private sector. As regards the supervisory authority for the public sector there was a federal delegate and one delegate for each Land which received notifications and kept the registers which were open to the public.
The supervisory authority in the public sector could turn to government and parliament and report on certain matters which give rise to concern.

For the private sector each land had its supervisory authority which could act following complaints or following indications in for example the press. In certain cases it could also investigate on its own motion. If complaints were made, measures were undertaken in order to reconcile the parties which were also informed of the legal remedies available. The supervisory authority could in certain circumstances intervene and for example forbid processing if there was a breach of security.

The Danish delegation explained that the supervisory authority in Denmark was an independent body which did not receive instructions from any minister.

In Denmark there was an act for the private sector and one for the public. In the private sector storing of data could take place if this was a natural part of a company’s activities. Storing of sensitive data could, however, only take place if permitted by law.

The supervisory authority could act on its own motion or on complaint and could require a private company to give any information deemed necessary. It could, furthermore, make inspections and this without a court order. If it was discovered that a company did not comply with the law it could be ordered to correct or erase data. Should the file keepers not comply with the order the law provided for the possibility of issuing fines or for punishment by imprisonment.

The decisions of the supervisory authority were final and could only be annulled by the courts. The supervisory authority issued an annual report to Parliament with a description of the principal cases arisen during the year.
In the public sector there was a general notification system for normal files whereas in the area of confidential or sensitive data a special set of guidelines had to be issued by the file keeper on which the supervisory authority gave its opinion. Should the supervisory authority not agree with the file keeper the final decision would be taken by the competent minister.

Also in the public sector the supervisory authority had the power of making inspections and if it was discovered that a public authority did not comply with the law the supervisory authority could report to the political authority responsible. Should a public authority not follow the recommendations issued by the supervisory authority this would be included in the annual report to parliament.

34. The Belgian delegation explained that the Belgian bill on data protection envisaged the creation of a commission with the power of issuing motivated opinions within a certain time limit. The opinions could be issued ex officio or following complaints. The supervisory authority could also carry out enquiries. In the case where the supervisory authority could not succeed in reconciling the parties it could suggest to the parties to bring the case before the courts.

35. The United Kingdom delegation explained that the supervisory authority in the United Kingdom was independent of government and parliament and had a statutory duty to enforce the law on data protection involving registering of about 130,000 data users and ensuring that the principles of data protection were adhered to. Non adherence could lead to de-registration and could be the subject of penal sanctions.

The supervisory authority could also issue guidelines and agreed codes of conduct with specific sectors. The supervisory authority could make investigations on its own motion but did not have any powers to seize documents. It could, however,
apply for a search warrant. Any notice of enforcement was subject to appeal to the data protection Tribunal with a further appeal to the courts.

In the United Kingdom no distinction was made between the private and public sectors nor was there a distinction between sensitive and non-sensitive data. The registration which took place in the United Kingdom was only a recording of the purposes for which files were kept and did not involve any authorization or declaration by the supervisory authority that the file was legitimate or not.

36. The Portuguese delegation explained that in Portugal a distinction was made between three categories of data:

1. those data exempted from notification, for example data for personal use and data for normal commercial use;

2. those data which were not exempted and which were not sensitive where advance notification should be made, and

3. sensitive data where an advance authorization was necessary.

In Portugal the supervisory authority was a public body independent from government and parliament. It could give opinions on public sector files and authorize sensitive data files and register files not exempted from notification. It could denounce all infringements which could be the subject of severe penal sanctions.

37. The Netherlands delegation explained that the supervisory authority in the Netherlands was an independent body the members of which were appointed by the Queen. The task of the supervisory authority was to ensure that the private as well as the public sector respected the law.
In the Netherlands there was a general notification system for the public and private sectors with clearly defined exceptions. All non-exempted files would have to be registered before they could be operational.

Should a file not have been registered the supervisory authority, which was only an advisory body, could draw up a report with the possible consequences of criminal prosecutions being undertaken. The supervisory authority could investigate on complaint or on its own motion and the user of files were obliged to give information without any recourse to principles of confidentiality. An investigation could lead to a recommendation to the keeper of a file and in a yearly report to Parliament there would be an indication of the investigations carried out and the recommendations given.

Codes of conduct established by specific sectors were sent to the supervisory authority which gave its opinion without, however, any legal consequence.

In the Netherlands there was a risk liability for the keeper of the file which had as a consequence that recommendations from the supervisory authority were complied with.

38. The Luxembourg delegation explained that in Luxembourg all data files, private and public, had to be authorized. This was a complex procedure but a guarantee for transparency as all information was contained in the register which could be consulted by everybody.

Before any file could be operated a consultative committee would give a motivated opinion. Following authorization the minister responsible could request investigation to be carried out and there were legal sanctions against those who tried to prevent officials from carrying out an investigation.
Sanctions which could be severe were foreseen for non-authorized use or use going beyond the authorization.

39. The Italian delegation indicated that it had basically opted for a notification system to the supervisory authority. The supervisory authority had a number of powers and could seek enforcement through the courts.

At the end of the meeting the Belgian delegation reserved its position on any conclusions arrived at during the meeting of the Working Party.
Discussion paper on Chapters II and III

1. Introduction

The need for a harmonization of data protection law is generally accepted. However, the degree of harmonization which is required and the methods to be applied in it have been the subject of discussion.

It is agreed that any harmonization should satisfy the needs of the developing internal market. Therefore, it should allow and guarantee a free flow of data and a high level of protection for data subjects throughout the Community.

Any effective protection scheme should be based on an appropriate balance between national legislation and Community measures.

2. General approach

It is agreed that the basic principles for data protection set out in the Council of Europe Convention of 28 January 1981 should be supplemented by other principles.

Among these principles there should be new principles, i.e. dealing with supervisory authorities, liability and transfer of data to third countries.
A large majority of the delegations is prepared to accept further principles in order to ensure a sufficient degree of harmonization of the rules implementing the basic principles of the Convention. These further principles could be of a substantial and a procedural nature.

The principles of the Directive would have to be sufficiently precise in order to limit their scope of interpretation. At the same time, it is agreed that the Member States should be allowed sufficient flexibility to choose the appropriate means for implementing the principles in each particular context, given their wide area of application.

Each Member State should be allowed the possibility to go beyond the level of protection agreed upon in the Directive, on condition that this possibility would be used for compelling reasons only and that the relevant measures would be necessary, proportionate and non-discriminating.

The precise scope of Article 1(2) and its relationship with Article 6(2) need further study.

3. Substantive principles

The basic principle of fair collection laid down in Article 16(1)(a) needs to be supplemented by other principles, i.e. referring to the provision of information at the time of collection.

The basic principle of lawful processing needs to be supplemented by other principles laying down the basic conditions for such processing, regardless of the sector in which the processing takes place.

In this context the processing of personal data should only be lawful:
- with explicit consent of the data subject, or

- where necessary for the execution of a contract with the data subject, or

- where necessary for the fulfillment of a legal obligation, or

- where necessary for the execution of a public function or duty, or

- where necessary to safeguard the legitimate interest of the controller, on condition that the interest of the data subject does not prevail.

Communication of personal data to third parties should be lawful on the same grounds and also:

- where necessary to safeguard the legitimate interest of a third party or the general public, on condition that the interest of the data subject does not prevail, or

- where necessary to protect vital interests of the data subject.

Special provisions might apply to processors and to communication of data for special purposes like direct marketing or for research and statistics.

The possible need for other substantive principles would require further study. However, it is agreed that the nature of the data should always be taken into account and that sensitive data might require more restrictive criteria.

4. Methods of application

The Directive should allow different mechanisms for implementation and application of the principles agreed upon, taking into account the nature of the data and the situation of
the data subject as well as the special characteristics of each sector, provided that certain minimum requirements are respected.

With regard to notification procedures it is agreed that a selective approach is needed, which should be based on an evaluation of the risks of data processing.

A large majority of cases should be exempted from notification either in general or under certain specified conditions. These conditions could be the subject of specific provisions, standard rules or approved codes of conduct.