OUTCOME OF PROCEEDINGS

of : Working Party on Economic Questions (Data Protection)
on : 19 March 1992

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

1. The Working Party on Economic Questions (Data Protection) held its 13th meeting on 19 March 1992 during which it continued its examination of the proposal for a Council Directive concerning the protection of individuals in relation to the processing of personal data. The meeting was devoted to discussions of the following items:

I. Definition of sensitive data - criteria of sensitivity.

II. Point 4 of Working Document No 15.

III. Criteria for lawful processing and communication (annex to document 10503/91).

1. Definition of sensitive data - criteria of sensitivity

a. Definition of sensitive data

2. Discussing the categories of data which would merit a particular protection and taking its point of departure in the special categories of data listed in Article 17 paragraph 1 of
the draft directive, the Working Party noted that a large number of delegations could accept the list of data set out in this article.

3. For the Belgian, Danish and Portuguese delegations the list in Article 17(1) should, however, not be considered as an exhaustive list but as a minimum list (examples) giving the Member States the possibility to enlarge the list according to specific national needs. The Luxembourg delegation and the Representative of the Commission expressed doubts as to the approach expressed by the three delegations as it would run counter to the purpose of the directive of harmonizing national provisions.

4. The French delegation could also accept the list set out in Article 17(1) but invited the Working Party to reflect on the suggestions it had made in its Working Document No 12 to also provide a particular protection for national identification numbers and population records; also criminal convictions should, in the French delegation's view, have a reinforced protection but the French delegation admitted that it was difficult to assimilate criminal records with the sensitive data listed in Article 17(1).

For the Belgian delegation criminal convictions and identification numbers were to be considered as semi-sensitive data which need an increased protection although not at the same level as sensitive data.

5. The German delegation explained that in Germany no distinction was made between sensitive and non-sensitive data. Although it did therefore not think Article 17(1) was indispensable, it could accept it provided that Article 17(2) permitting Member States to grant derogations from paragraph 1 was maintained.
6. The Greek delegation indicated that the existence on international level of several texts on the same question could lead to a number of problems; it was therefore in principle against having a text different from Article 6 of the Council of Europe Convention. The Greek delegation was in particular opposed to the inclusion in Article 17(1) of data relating to trade union membership.

7. Also the Irish delegation preferred to confine sensitive data to the grouping set out in Article 6 of the Council of Europe Convention. It could, however, accept the clarification made in Article 17 in respect of "ethnic origin" and "philosophical beliefs". The Irish delegation suggested that special consideration be given to data collected by social helpers.

8. The United Kingdom delegation reserved its position on the list of sensitive data set out in Article 17. In the United Kingdom delegation's view certain data were not sensitive in all circumstances but could become so by the purpose to which they were put. The United Kingdom delegation agreed, however, that the list of data set out in Article 17(1) were likely to be used for sensitive purposes.

b. Criteria for sensitivity

9. Further to the list of sensitive data - this being exhaustive or not - a number of delegations agreed that certain general rules be established to protect individuals against certain types of processing of data which were not sensitive from the outset but could become sensitive by the processing they underwent.

II. Point 4 of Working Document No 15

10. In its Working Document the German delegation had indicated that in the private sector compulsory registration would seem in principle to be justified for the types of data
listed in Article 17(1). The idea of waiving compulsory registration if the individual concerned consents to the processing should, however, in the German delegation's view be taken up. Otherwise, all medical practitioners, insurance companies and offices handling medical expenses for example, would be obliged to register. It would also, in the German delegation's view, be reasonable not to require compulsory registration in cases where the individual concerned consents in connection with his employment to having membership of a trade union or religious group recorded in a data file.

11. The French delegation recalled that it had proposed in its Working Document No 12 that processing of sensitive data should be subject to a prior authorization. In the French delegation's view such a prior authorization could not be replaced by a simple notification. What the French delegation was prepared to consider was whether as an alternative to prior authorization by the competent supervisory authority a prior authorization could be given by the legislator.

In the case where the data subject had given his express written consent there might not be a need to impose a prior authorization and a more simple system could be envisaged including, however, a notification - or maybe limiting the cases where processing could be carried out to certain precisely delimited cases.

12. The Netherlands delegation recalled that it could not accept the prior authorization system proposed by the French delegation but that it was prepared to seek for a protection system equivalent to a prior authorization.

As to the question whether consent of the interested individual could be a basis for processing sensitive data, such a consent would, in the Netherlands delegation's view not be enough. Even if a consent had been given it should always be possible to withdraw a given consent and thus prevent a processing of sensitive data.
13. The Belgian delegation agreed that a simple notification system would not suffice. In the Belgian delegation's view processing of sensitive data should only be permitted

- when the law so provided;
- if the supervisory authority had given its authorization;
- when the data subject gives his consent and the law did not prohibit it.

14. The United Kingdom delegation recalled that in its opinion a notification system did not help to discover who held data or help authorities in their controlling functions. The United Kingdom delegation favoured the approach laid down in the Council of Europe Convention according to which the Member States should provide an adequate protection of sensitive data. In the United Kingdom the same protection was given to sensitive and non-sensitive data and although the law gave certain powers to protect certain data these powers had not been used.

15. The Danish delegation recalled that it had sympathy with the proposals made by the French delegation as the existing system in Denmark in respect of sensitive data was quite similar to that proposed by the French delegation.

16. The Irish delegation explained that in Ireland sensitive data was subject to a prior authorization and that processing of sensitive data as defined in Article 6 of the Council of Europe Convention was refused by the supervisory authority unless it was convinced that the privacy of individuals was protected. The Irish delegation agreed with the German delegation that one should avoid unnecessary notification for, for example, employers holding information on health or religion. For the Irish delegation the importance did not lie in the fact that for example health data were collected but rather in the way it was used, and in this connection it was
important that the supervisory authority had adequate powers to intervene in the few cases where an infringement had taken place.

17. The Luxembourg delegation indicated that it had a preference for the proposals made by the French delegation for a prior authorization by the supervisory authority; if consent was to form a basis for the processing of sensitive data then the conditions under which and for what the consent was given had to be clearly specified.

18. The Italian delegation had always been in favour of a supervisory authority with real powers and in this sense the proposals by the French delegation were interesting to the Italian delegation as they gave extra guarantees than a simple notification. One would, however, have to examine clearly under which conditions a prior authorization was given. Also the conditions under which a consent by the individual concerned could form a basis for the processing of sensitive data would have to be clarified.

19. The Greek delegation proposed that processing of sensitive data should be permitted only if there was a prior written consent by the person concerned as well as a prior authorization by the supervisory authority and the processing was necessary for the accomplishment of certain functions.

III. Criteria for lawful processing and communication (Annex to doc. 10503/91)

i) Lawful processing

20. Discussing the additional five criteria to supplement Article 16(1)(a) in order to lay down the basic conditions for processing set out on page 18 of doc. 10503/91, a number of delegations indicated their agreement on these principles.
21. The French delegation could agree to the first four principles set out on page 18 of doc. 10503/91 but felt that the fifth principle was worded in too vague a manner. This view was shared by the Belgian delegation.

22. The United Kingdom and Irish delegations expressed doubts as to the approach taken in doc. 10503/91 that processing was unlawful unless the principles set out on page 18 were fulfilled. In these delegations' view the approach should rather be that the processing was lawful but could become harmful under certain conditions. In the Irish delegation's view the problems did not arise so much in the processing of data but rather in relation to the communication of data.

1) Communication of data

23. On page 18 of doc. 10503/91 two criteria for lawful communication were set out in addition to those for lawful processing.

24. Commenting on these two additional criteria, the French delegation indicated that in its view the opposite approach than that set out in doc. 10503/91 should be used. Instead of having the flexible system for communicating data as suggested in doc. 10503/91, there should be a set of stricter rules and in this context the French delegation suggested limiting the criteria for lawful communication to the following:

- the data subject had given his explicit consent;

- the communication was necessary to fulfil a legal obligation;

- the communication was necessary for the execution of a public function or duty.
25. Also the Greek delegation expressed doubts as to the need for these two additional criteria for lawful communication, set out on page 18 of doc. 10503/91.

26. The Irish delegation indicated that the first of the two additional criteria for lawful communication needed to be clarified in order to avoid litigation.

27. A number of delegations did not share the view that the two additional criteria for lawful communication were unnecessary. In these delegations' view such additional criteria had to be mentioned because of the involvement of a third party when data were communicated.
OUTCOME OF PROCEEDINGS

of: Working Party on Economic Questions (Data Protection)
on: 18 June 1992

No. prev. doc.: 5490/92 ECO 50
No. Cion prop.: 8460/90 ECO 158 - COM(90) 314 final SYN 287 - 288

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

1. The Working Party on Economic Questions (Data Protection) held its 14th meeting on 18 June 1992 during which it continued its examination of the proposal for a Council Directive concerning the protection of individuals in relation to the processing of personal data. The meeting was devoted to:

   I. The role of self-regulation in the scheme of data protection.

   II. The scope of the Directive: - exceptions (Article 3 paragraph 2).

I. The role of self-regulation

2. The Working Party’s discussion of the role of self-regulation was based on Working Document No 16 drawn up by the Netherlands delegation. In introducing its document and answering a number of questions put forward by delegations, the Netherlands delegation explained that it was not possible in codes of conduct to derogate from the law. The purpose of codes of conduct was to interpret or supplement the law on data...
protection and any derogation to that law would have to be done by a new law. Such laws did indeed already exist and a further one was under preparation.

As regards the declarations issued by the Registration Chamber to the effect that a code of conduct was in conformity with the provisions of the data protection Act, such a recommendation would naturally play a role if a case was brought to court. It would not, however, prevent the judge from ruling that the code of conduct did not reflect a correct interpretation of the Act of data protection. The Netherlands delegation in this context explained that proceedings before the court were civil proceedings and no penal sanctions were foreseen.

As to assessing whether the applicant applying to the Registration Chamber for a declaration that the code of conduct conformed with the provisions of the data protection Act was sufficiently representative, the Netherlands delegation indicated that this was exactly one of the elements the Registration Chamber considered before giving its declaration.

As regards the question of defining the sector for which the code would apply, this did in most cases not give rise to problems.

The Netherlands delegation finally indicated that it was in favour of Article 20 of the draft Directive but wondered whether, as was the case in the Netherlands, there should not be the possibility of laying down binding regulations for a certain sector as a sanction for inadequate or ineffective self-regulation. The Netherlands delegation also wondered whether codes of conduct on a Community level should not be provided for.

3. The Irish delegation explained that the Irish system in respect of codes of conduct went further than the system applied in the Netherlands because the codes of conduct would
have the force of law. In Ireland the supervisory authority would encourage different sectors to establish codes of conduct containing more detailed rules than the law on data processing. Once established, the code of conduct in a specific sector would be submitted to the supervisory authority who would approve or enter into negotiation in order to improve the codes before approval. The approved code of conduct would then be sent to the Ministry of Justice who would put it before the two houses of Parliament. If passed by Parliament the code of conduct would have the force of law.

No codes of conduct yet existed in Ireland but a number of sectors were preparing such codes.

4. The German delegation explained that in Germany there were a number of types of codes of conduct, some having the character of statutes of law containing rules for lawyers and doctors, others being voluntary codes of conduct negotiated between the authorities and sectors like banks and credit institutions. Whereas the statutes of law for lawyers and doctors were legally binding, the voluntary codes had no direct legally binding force and could be revised if necessary following, for example, a ruling by a court.

The German delegation considered codes of conduct as a means of interpreting the law but expressed concern that certain sectors might not take the initiative to draw up such codes.

5. The United Kingdom delegation explained that in the United Kingdom five codes of conduct, with no statutory backup, existed. They had been drawn up on the basis of a totally voluntary arrangement between the Registrar and different organisations in order to give indications as to how the data protection Act should be interpreted. Even if the codes of conduct had not got the force of law, they could be, and as a matter of fact had been, used before the courts.
The United Kingdom delegation, like the Netherlands delegation, supported Article 20 of the draft Directive which it considered a useful and flexible means of ensuring compliance with data protection principles.

6. The Belgian, Danish, French and Luxembourg delegations indicated that codes of conduct did not exist in their countries. The Danish delegation did, however, understand the interest certain codes of conduct could have, but stressed that codes of conduct could only be non-binding rules. The areas where codes of conduct could be a possibility were only those where there was no need for binding rules.

7. Comparing the approach in the Netherlands, which was to establish codes of conduct in order to replace laws, with that in Ireland, which was to arrive at legally binding rules, the Representative of the Commission queried whether industry might not express misgiving if codes of conduct were to be binding.

II. The scope of the Directive: exceptions (Article 3 paragraph 2)

8. The discussions of the Working Party of this point was based on Working Document No 18 from the Belgian delegation and Working Document No 19 from the Danish delegation, concerning respectively statistical data and research files.

9. Addressing the question of research files in particular, the German delegation indicated that in their opinion such files should not be covered by the general framework Directive but rather by a sectoral Directive.

10. The Belgian delegation addressing also the question of research files, explained that when discussing the Bill of data protection in Belgium the question of research files had arisen. On the basis of this discussion it was now being considered whether to enter an amendment in the Bill to cover research files. As such files gave rise to specific problems
which needed careful consideration, the Belgian delegation as the German delegation, felt that it might be useful that they be dealt with in a sectoral directive.

11. The French delegation indicated that it had understanding for the difficulties explained by the Danish and Belgian delegations in their documents. As a provisional view, the French delegation felt that it might be advantageous for the specific problems raised by the two delegations to be dealt with in the general directive itself avoiding other negotiation at some later stage. The French delegation recognized, however, that such an approach might delay the adoption of the Directive which it did not want.

12. Also the Greek delegation agreed with the concerns expressed by the Belgian and Danish delegations in their documents. In the Greek delegation's view consideration should furthermore be given to the area of the delivrance of medical certificates which had given rise to specific problems in Greece.

13. The United Kingdom delegation supported the anxieties of the Danish and Belgian delegations. The United Kingdom delegation was, however, not sure whether the statistical data and research files should be excluded altogether from the general Directive or should be covered by specific control clauses.

14. The Italian delegation stated that in its opinion there should be exceptions for statistical data and research files but these should not be total exceptions. In the Italian delegation's view certain problems might arise for research files in the cases where these files were used also for other purposes. The Italian delegation also wondered whether Amendment No 60 proposed by Parliament would be compatible with Article 9 of the Council of Europe Convention.
15. The Netherlands delegation agreed with the Italian delegation as to the doubt on the compatibility with the Council of Europe Convention. Referring specifically to Article 5e of that Convention, the Netherlands delegation queried whether keeping files for any unlimited time, with the aim that this data might possibly be used for research purposes at some later time was compatible with this Article.

In the Netherlands a patient had the right to request that his medical file be destroyed. If such a request was not made it would be destroyed after 5 years. During these 5 years the data could be used and passed on to a research body.

16. The Danish delegation, referring to Amendment No 60 by Parliament, which would allow data instead of being erased to be transferred to archives, stated that this amendment, if followed, would not suffice to meet its concerns as problems would remain in respect of the question of the accessibility of research files to other files. The maintenance of an obligation of consent in these cases would, in the Danish delegation's view, ruin all research possibilities.

Addressing the question raised by the Netherlands on Article 5e of the Council of Europe Convention, the Danish delegation explained that it was difficult to say when files no longer served their purpose. In Denmark medical data were erased 10 years after the patient's death.
Opinion on:

- the proposal for a Council Directive concerning the protection of individuals in relation to the processing of personal data,

- the proposal for a Council Directive concerning the protection of personal data and privacy in the context of public digital telecommunications networks, in particular the integrated services digital network (ISDN) and public digital mobile networks, and

- the proposal for a Council Decision in the field of information security (1)

(91/C 159/14)

On 2 October 1990 the Council decided to consult the Economic and Social Committee, under Article 100 a and Article 235 of the Treaty establishing the European Economic Community, on the abovementioned proposals.

The Section for Industry, Commerce, Crafts and Services, which was responsible for preparing the Committee's work on the subject, adopted its Opinion on 3 April 1991. The Rapporteur was Mr Salmon.

At its 286th plenary session (meeting of 24 April 1991), the Economic and Social Committee adopted the following Opinion by 80 votes to 13, with four abstentions.

1. General principles

1.1. The package of proposals presented by the Commission is designed to facilitate and encourage the free movement of personal data while strictly protecting the privacy of the individual.

1.1.1. The proposals seem justified in the light of the need to meet a number of basic requirements, and in particular those laid down in Council of Europe Convention 108 of 28 January 1981, and in subsequent sectoral recommendations, for the protection of individuals with regard to automatic processing of personal data.

1.2. Personal data undergoing automatic processing must be:

- collected and processed fairly and lawfully,

- stored for specified, legitimate purposes, and used in a way compatible with these purposes,

- adequate, relevant and not excessive in relation to the purposes for which they are stored,

- accurate and, where necessary, kept up to date,

- preserved in a form which permits identification of the data subjects for no longer than is necessary for the purpose for which the data are stored.

1.2.1. Personal data revealing racial origin, political opinions or religious or other beliefs, as well as personal data concerning health or sexual life, may not be processed automatically unless domestic law provides appropriate safeguards. The same applies to personal data relating to criminal convictions.

1.3. Any person must be enabled:

- to establish the existence of an automated personal data file, its main purposes, as well as the identity and habitual residence or principal place of business of the controller of the file,

- to obtain at reasonable intervals and without excessive delay or expense confirmation of whether personal data relating to him are stored in the automated data file as well as communication to him of such data in an intelligible form,

- to obtain, as the case may be, rectification or erasure of such data if these have been processed in violation of the provisions of domestic law giving effect to the basic principles set out in Articles 5 and 8 of the Convention 108,

- to have a remedy if a request for confirmation as the case may be, communication, rectification or erasure as referred to in paragraphs b) and c) of Article 8 of the Convention is not complied with.
Accordingly, any person who orders or carries the processing of personal information must under­take to take all the necessary precautions to preserve the security of the data and to prevent it being distorted, damaged or communicated to unauthorized third par­ties.

These principles are mainly covered by Articles 17 and 18 of the proposed general Directive (SYN 199).

The fact that five Member States have no legislation of this type (notwithstanding Article 8 of the European Convention on Human Rights) is the chief cause for concern.

It is regrettable that the seven sectoral recommenda­tions already drawn up by the Council of Europe are not mentioned with a view to the possible abrogation of sectoral provisions.

The overall package must ensure a high level of protection and, more particularly, must not lower the level already pertaining in those Member States with relevant legislation. The Directive further clarifies and supplements the abovementioned Convention 108. It adds additional specifications of the rights of data subjects (e.g. in Article 14), and clarifies the conditions under which processing is lawful (Chapters II and III); in some cases these rest on the rights of the data subject (information, consent, etc.). The Directive also specifies conditions of notification and lastly lays down certain restrictions and provides detailed coverage of the question of security and the transfer of data to third countries.

It is not easy to assess the practical impact of additional provisions and restrictions on the level of protection pertaining in the Member States.

The provisions combine basic legal concepts differing national legislation (mainly French, German and Dutch) which are open to differing interpretation. Furthermore, the Member States are given relatively broad powers in deciding how to implement the Directive.

In practice, it is thus difficult to gauge whether the package will increase the level of protection or simply intensify the differences. Certain reductions in the level of protection are clearly apparent: restrictions on notification, fewer constraints on the public sector. The co-existence of different notification systems is accepted.

1.5.4. The free movement of persons should mean a minimum level of uniformity between Member States as regards the obligations incumbent on bodies which process personal information, the rights of data subjects, and the provisions for exercising these rights.

1.6. It is also surprising—to say the least—that the obligations placed on the private sector could appear greater than those on the public sector (notification possibly required for the communication of data by the private sector, no such requirement for the communication of data between public authorities). Some of the general and specific provisions on individual rights are inconsistent (right to information, consent, opposition).

1.7. To appreciate the impact in the Member States and at European level of the three proposals submitted to the ESC, it is necessary to consider the other texts contained in COM(90)314 final.

1.7.1. The Committee would here draw the attention of governments to the following points concerning:

— the draft resolution of the representatives of the governments of the Member States of the European Communities meeting within the Council; the comments below on the public sector should also apply to those parts of the public sector which do not fall within the scope of Community law,

— the recommendation for a Council Decision on the opening of negotiations with a view to the accession of the European Communities to the Council of Europe Convention for the protection of individuals with regard to the automatic processing of personal data: in a case like the present where the protection of basic rights is at stake, it is going too far to empower the Commission to negotiate directly with the Council of Europe, replacing the seven Member States already represented on the consultative committee set up under Convention 108 and the other five Member States invited to adhere to it.
1.7.2. The Commission should join the consultative committee, though without infringing on the rights of the Member States by conducting the negotiations.


2.1. General comments

2.1.1. The Committee approves the aim and rationale of the proposal. Several ESC Opinions have called for serious consideration of the question of high-level data protection and a precise definition of the personal data which must be protected. This latter Opinion stressed that public mistrust, whether justified or merely the result of ignorance, could, if neglected, rapidly create a serious political obstacle to the introduction of efficient communications technologies.

2.1.2. It should however be emphasized that the aim of this protection is to guarantee, in the territory of each party, respect of individual rights and fundamental freedoms, and in particular the right to privacy with regard to the automatic processing of personal data, irrespective of nationality or place of residence.

2.1.3. The recitals refer to Council of Europe Convention 108. All the national laws hitherto adopted apply the general principles of data protection laid down in this Convention.

2.1.3.1. These principles are common to national laws, and the draft Directive and explanatory memorandum are also based on them. They are restated by the Committee at the start of this Opinion.

2.2. Specific comments

These comments seek to illustrate the problems raised by most of Directive SYN 287’s proposed additions and clarifications to the principles listed in Convention 108.

2.2.1. Article 1 — Object of the Directive

— The recitals refer to the European Convention on Human Rights and Council of Europe Convention 108, with a view to guaranteeing the individual's 'rights and fundamental freedoms, and in particular the right to the respect for privacy'. In the light of this, the Committee considers that the scope of the Directive should not be limited to the protection of privacy.

— Article 1(1) introduces the concept of 'data file', which fixes the scope of the Directive.

2.2.1.1. The concept seems too narrow: personal data can nowadays be processed in an expert system without necessarily having to be structured (integated data-bases).

2.2.1.2. Moreover, it is the 'purpose' of the processing which is crucial in data protection, and which establishes whether or not the collection of data is legitimate.

2.2.1.3. Accordingly, the Committee feels that the concept 'processing of personal data', rather than 'files', should be used to define the scope of the Directive.

2.2.1.4. The term 'processing' should therefore replace the term 'file' in Articles 3, 4, 5, 7, 8(1)(6)(8), 10 and 11.

2.2.2. Article 2 — Definitions

2.2.2.1. The Committee supports the decision to adopt the definitions contained in Convention 108. However the definition of 'depersonalize' is cleared up in the explanatory memorandum.

2.2.2.2. The explanation limits the scope of the definition, allowing further attention to be given to data which, although depersonalized by the producer, remain associated, after communication, with personal data from other processing.

2.2.2.3. Moreover, 'excessive effort' should be deleted, for a processing task requiring an excessive effort today may require no effort at all next year.

2.2.2.4. The Committee feels that manual files should also be covered; this should include collection of files, particularly when they are directly linked to automatic processing.

2.2.2.5. However, an obligation to notify the existence of all manual files would not be feasible.
2.2.6. The definition of processing should include a definition of collection.

2.2.7. The Committee considers that the independence of the relevant national authority is a useful check vis-à-vis Convention 108.

2.2.8. The defence of fundamental freedoms, and of privacy in particular, in information processing operations must require that the supervisory authorities are independent.

2.2.9. The distinction should not only be based on whether or not such enterprises engage in commercial activity.

2.2.10. Enterprises which have a monopoly or a public service concession as defined by Article 90 of the Treaty should be considered as being in the private sector, as far as the application of the rules applicable in that sector does not obstruct the performance, in law or in fact, of the particular tasks assigned to such enterprises.

2.2.11. In order to clarify the implementing provisions of the Directive the term ‘adequate level of protection’ should also be defined.

2.2.12. The definition should exclude the transfer of data within a body, where this is a necessary part of the processing.

2.2.13. The Committee endorses the proposed exemption.

2.2.14. The Committee considers that processing by trade organizations and charitable organizations should also be exempt.

2.2.15. Notwithstanding the proposed exemption for ‘sporadic use or a file temporarily’ could be dangerous. They would allow anyone to conduct highly sensitive but temporary operations without being subject to protection measures.

2.2.16. Furthermore, the term ‘adequate level of protection’ is surprising, as what is needed is equivalent protection on a case-by-case basis, depending on the category of data involved (cf. Convention 108).

2.2.17. Article 5 — Lawfulness of processing in the public sector

2.2.18. The Directive goes further than Convention 108 by seeking to establish criteria for deciding whether processing is lawful. These criteria appear inadequate or open to differing interpretations. The ‘legitimate interests of the data subject’ and the ‘serious infringement of the rights of others’ are two cases in point.

2.2.19. Moreover, the criterion of being ‘necessary for the performance of the tasks of the public authority’, even if laid down by law, is insufficient to legitimize per se the processing of personal data.

2.2.20. In large-scale applications whose design, programming and implementation can be very costly, risk analysis is done on a case-by-case basis long before the design stage, and not afterwards. Decisions made during the design of the data processing application must seek to minimize or eliminate any threat to the rights of the data subject, while reconciling the interests at stake.

2.2.21. Fear of the potential use which the authorities could make of immense data stores has triggered major public campaigns in some Member States.

2.2.22. At European level, research into telematic networks linking administrations or for use in the health sector has already given cause for concern.

2.2.23. Accordingly, the Committee considers that national supervisory authorities should be granted explicit powers of examination prior to the processing of particularly important or sensitive data.

2.2.24. Such controls should only be exercised selectively.

2.2.25. Provision should also be made for disclosure of the existence of data.
2.2.6. **Article 6 — Communication**

In the public sector: the comments on Article 5 concerning the transfer of data between public bodies are even more relevant here. Certain communications should be subject to prior control by the supervisory authority. Article 6(2) makes this a possibility, but leaves it to the initiative of the Member States. Moreover, the application of the Directive to European-level plans for administrative coordination involving the exchange of personal data means that case-by-case preliminary examinations are needed.

In the private sector: it is reasonable to leave the Member States to issue any authorizations. This being the case, the differing systems laid down for transfers between administrations and between private bodies seem unjustified.

By laying down systematic rules for the notification of the supervisory authority only in respect of public sector processing for communication purposes, the Directive assumes that this is the area of processing most likely to cause problems. This is not a proven fact.

2.2.7. In some Member States, the combined effect of Articles 5, 6 and 7 will be to reduce the level of protection, contrary to the objectives pursued by the Commission.

2.2.8. **Article 8**

2.2.8.1. Article 8 defines the conditions under which the processing of personal data in the private sector is considered lawful. The data subject must give consent, the processing must be carried out under a contract, and the data must come from 'sources generally accessible to the public'.

2.2.8.2. The term 'quasi-contractual relationship' is open to differing interpretations. 'A quasi-contractual relationship of trust' should not be interpreted too restrictively, as this would impede normal commercial activities. The term 'sources generally accessible to the public' is questionable and could even be dangerous.

2.2.8.3. The very existence of a wide variety of directories does not make it legitimate to use them indiscriminately.

2.2.8.4. More to the point, registers of births, marriages and deaths and electoral registers are all 'generally accessible' but should only be so for particular purposes and under precisely defined conditions.

2.2.8.5. The Committee therefore considers that reference to 'sources generally accessible to the public' should be used with extreme caution.

2.2.9. **Articles 9 and 10**

2.2.9.1. Unlike transfers between public authorities, the Directive obliges private sector operators to inform the data subject when a file is first communicated. The data subject also has the right to object to further communication or to any other processing. Exceptions are possible, but only with the authorization of the supervisory authority.

2.2.9.2. The principle is sound, but surely the information is redundant, and involves unnecessary cost if it has already been supplied when obtaining consent (Article 12) or collecting the data (Article 13).

2.2.9.3. Special consideration should be given to the communication of medical data, which should be subject to the agreement of the patient and only be communicated to doctors actually treating the patient.

2.2.10. **Article 11**

2.2.10.1. As in the case of the public sector (Article 7), systematic notification in the private sector is obligatory if the file data (the processed data) are intended to be communicated.

2.2.10.2. Notification should not be required in the case of communications made for reasons of security (restoration of data, back-up) or pursuant to a contract.

2.2.10.3. Rental of files for marketing purposes should however be subject to the agreement of the parties concerned.

2.2.10.4. Lastly and most importantly, the Committee considers that transmission of files pooled among members of professions (e.g. lists of bad debtors or the issuers of dishonoured bills of exchange, cheques, etc.) should be subject to both a priori and a posteriori control.
Articles 12, 13 and 14

These Articles list the rights of data subjects on the provisions of Convention 108, the addition of certain specific rights currently contained in national legislation relating to the data subject's right to be informed and to oppose. The directive also incorporates Article 2 of the French Law on the automatic processing of Personal data defining the sub-profile which is not used elsewhere.

However, some of these rights deserve to be applied more flexibly and more specifically in the light of the problems mentioned in 2.2.9.

Article 14(4) should specify that in all cases the data must be communicated by a doctor.

Lastly the Committee considers that the principle of cost-free right of access should be spelt out, particularly for real-time data access.

Article 15

Possible reasons for granting exceptions to the right of access include 'paramount economic and financial interest of a Member State or of the European Communities' (e.g. in matters of taxation or exchange controls), and 'an equivalent right of another individual to the rights and freedoms of others'. The latter covers economic freedoms (business and commercial secrecy).

In some Member States, these exceptions could lower the level of protection to a dangerous level.

In the Committee's view the application of these exceptions should be subject to control by the national data protection authorities, and this should ensure the private sector.

Article 16

Article lists the main principles on data quality contained in Convention 108. It deserves a more prominent place in the Directive.

Article 17 — special categories of data

Committee approves the use of the provisions of Convention 108 as regards sensitive data. Derogations should be subject to specific regulations.

Article 18

Article 18 provides a more detailed version of the provisions of Convention 108. Although it obliges the controller of the file to guarantee security and confidentiality, the controller may take into account 'the state of the art in this field, the cost of taking measures ...'. This seems dangerous, and will lower the level of protection in some Member States.

The technical means of protection used should of course be proportional to the risks (from the point of view of the person concerned), but should not depend on cost.

Either one has the means of protection and uses them, or one has not and does not. The regulatory power which the Commission confers on itself here could give rise to concern. The Commission should instead be helping to see that reasonably priced technical security devices are available on the market (the security market currently encourages the production of expensive systems specifically for the armaments and banking sectors).

Article 19

Article 19 provides for possible derogations for the press and the audiovisual media.

However, in the Committee's view these derogations should only apply to provisions of the Directive which clash with rules on freedom of information.

Article 20

Article 20 requires Member States to encourage business circles to assist in the drawing-up of European codes of conduct or professional ethics. The draft Directive borrows certain data protection provisions from national law (e.g. United Kingdom, Netherlands). It should be noted, however, that the legal scope of national provisions varies considerably. While it is sensible to cater for any implementing problems in particular sectors or processing categories (as have the Council of Europe, the international conference of data protection ombudsmen, and national authorities in, for example, the UK and France), the
draft Directive goes further in giving the Commission regulatory powers.

2.2.17.2. The formulation of these codes should take account of the comments made in 2.2.11. They should be subject to approval by the European data protection authority, and should not come under the regulatory powers of the Commission.

2.2.18. Articles 21, 22 and 23

The Committee endorses these Articles, which specify that compensation must be provided for any damage suffered, and that the Member States must make provision for criminal sanctions. Processing by a third party on behalf of the controller of the file must be governed by a written contract stipulating the responsibility of the third party with particular regard to confidentiality and security.

2.2.19. Articles 24 and 25

Transfer of personal data to third countries

2.2.19.1. The Committee considers that the Directive should adopt the principle of 'equivalent' protection, as laid down in Convention 108.

2.2.19.2. The proposed wording fails to draw the practical consequences of the draft Directive on the protection of personal data in telecommunications networks. Aside from the principles of Convention 108, the way to obtain effective equivalent protection at international level is to adopt practical common measures.

2.2.19.3. To be relevant, these measures must be devised for processing categories with common characteristics and common data protection problems.

2.2.19.4. Moreover, a procedure is needed for devising effective, specific protection measures for these common categories when their data are transferred to third countries. This procedure should involve the independent European data protection authority.

2.2.19.5. Equivalent protection for transfers to third countries could be based on the same pragmatic method. At all events, the European data protection ombudsmen have so far not signalled any particular problems in this area. This is why the Committee considers that the proposed procedure is inappropriate.

2.2.19.6. The Committee considers that the Directive should be empowered to conduct a prior examination of particularly sensitive processing operations (whether private or public), and to decide as they proceed which categories of processing do not impinge on the rights of the data subject and therefore do not need supervision.

2.2.19.7. Moreover, a procedure is needed for devising effective, specific protection measures for these common categories when their data are transferred to third countries. This procedure should involve the independent European data protection authority.

2.2.20. Article 26

2.2.20.1. This Article obliges each Member State to set up an independent supervisory authority with investigatory powers and powers of intervention.

2.2.20.2. In the light of the comments in 2.2.6 and 2.2.10, the Committee considers that this authority should be empowered to conduct a prior examination of particularly sensitive processing operations (whether private or public), and to decide as they proceed which categories of processing do not impinge on the rights of the data subject and therefore do not need supervision.

2.2.20.3. The authority should conduct this examination within the Member States with consultation of the parties concerned (companies, trade unions, administrative bodies, consumer associations, trade organizations, and so on).

2.2.20.4. It should be possible to appeal against the authority's decisions.

2.2.20.5. Moreover, it would be dangerous if these authorities were in practice to be undermined by the regulatory powers of the Commission, should the comments on Articles 27 and 28 go unheeded.

2.2.21. Articles 27 and 28

2.2.21.1. The draft Directive provides for the establishment of a working party on the protection of personal data, made up of representatives of the national supervisory authorities, to advise the Commission on data protection issues in the EC and third countries. Its advisory duties should include following up the implementation of the Directive and its adaptability to technological change.

2.2.21.2. As in the case of the national authorities, the working party should consult the relevant bodies.

2.2.21.3. However, the working party does not need to be fully independent. Its chairman will not be elected, but will be a representative of the Commission.

2.2.22. Articles 29 and 30

2.2.22.1. These Articles empower the Commission to adapt the Directive to the specific characteristics of
the interests of consistency with the general Direc-
tive (SYN 237), the Directive should only deal with
international telecommunications services so as to
standardize their operation in all Member States,
(b) the effect of data protection on the design of
specific equipment which is to move freely between
Member States (joint technical specifications),
— it should not include provisions which by their
nature ought to have been included in the general
Directive, i.e. Articles 4, 5 and 6 on the purpose and
length of storage and rights of subscribers.

3.2.1. Specific principles

3.2.1.1. The Committee considers that Articles 7
and 8 on the confidentiality of communications and the
technical consequences thereof (especially as regards
the encryption of radio communications) are relevant.

3.2.1.2. Protection must be effective and not
'adequate' [Article 8(1)], and it is dangerous in this
respect to refer to the 'state of the art' or the cost of
security, as proposed in the general Directive.

3.2.1.3. Another principle which should be included
is that, notwithstanding the questions of payment,
anonymous access to networks should be possible with
a view to guaranteeing the freedom of thought and
communication. Examples here include public phone
booths operated by coins or prepaid non-personal cards
and French videotex. (Cf. 1989 Berlin resolution of the
International Conference of data protection ombuds-
men, which stated that whatever the problems of billing
may be, the multiple links between networks demand
that anonymous access be made technically possible.)

3.2.1.4. A third specific principle could be to ban (a)
listening to or recording a private conversation without
a person's consent and (b) transmitting or recording
the picture of a person taken in a private place without
his or her consent. This principle would form the basis
for the technical provisions proposed in Article 15 with
regard to loudspeakers and recording equipment—pro-
visions which may seem arbitrary.

3.2.2. Article 4(2) on the electronic profiles of sub-
scribers: the outright ban is an extreme solution. Tel-
communications operators should be able to carry out statistical surveys for commercial or network-planning purpose, but abuses should not be permitted.

3.2.2.1. For example, it would be unreasonable, unless the client has previously approached the firm, to propose the purchase of an answering-machine to a client who often fails to answer incoming calls.

3.2.2.2. Before any decision is taken, this matter too should be examined by the European-wide coordinating body for data protection officials.

Services affected by the Directive

3.2.3. Directories

3.2.3.1. Although the question of directories is raised in Article 4 in connection with the processing of data, the problem has in fact been dodged, unless the Commission considers it dealt with in Article 8(1)(b) of the general Directive.

3.2.3.2. Under Article 8(1)(b) there are to be no specific safeguards with regard to data coming from sources 'generally accessible to the public' whose processing is intended solely for the purposes of 'correspondence'.

3.2.3.3. For example, there are to be no safeguards on the use of data from directories for canvassing by phone. This is unacceptable.

3.2.3.4. The Committee considers it vital that the question of telecommunications directories be tackled in the Directive.

3.2.3.5. The Directive should specify the conditions under which these data may be published. Non-inclusion in a telecommunications directory should be free of charge and should not have to be justified. The content (identification) of the data should not reveal the subscriber's sex unless the subscriber so wishes or make access to the home less safe. Accessing procedures, should guard against unauthorized downloading from electronic directories, etc.

3.2.4. Articles 9-11 — detailed billing

3.2.4.1. Detailed bills listing the numbers called from a particular telephone are highly confidential. Mindful of the delicacy of this issue, but also of the need for this information to check the accuracy of bills, the

Committee feels that full and detailed bills listing the numbers called should only be provided to subscribers who ask for them.

3.2.4.2. For their part, telecommunications operators should widely publicize this innovation, and announce their policy of anonymous payment in public hearings.

3.2.5. Articles 12 and 13: identification of the calling line

3.2.5.1. The first two paragraphs are correct. However, it should be explicitly stated that non-identification should not cost extra.

3.2.5.2. Article 12(3) deals with how a normal subscriber may be identified by another subscriber with equipment for displaying the calling line. The technical description of this situation seems inaccurate and the proposed safeguard inadequate.

3.2.5.3. The problem here is the link between subscriber and his/her exchange, which may be either digital or analogue. Identification of a normal subscriber will constitute a very big change for these subscribers. This is why it is not sufficient simply to notify them of this change. Having to agree to the identification of their line is a guarantee that subscribers are being properly informed. Subscribers who accept identification must retain the right to decide otherwise at short notice.

3.2.5.4. At all events, under the Commission proposal, the subscriber called will always be able to receive unidentified calls.

Article 13(3)

The meaning of this sentence is unclear. There is a Community plan—which has not yet been put into effect—to standardize emergency numbers in the event of, for example, fire. However, emergency assistance will remain a national preserve. It is thus unclear whether this derogation from the rule eliminating identification of the calling line should be operational on a Community-wide basis—it should remain a national preserve.

3.2.6. Article 14 — forwarding of calls

3.2.6.1. The first paragraph poses no problem in principle. However, the feasibility of obtaining the

91
This would seem to be too restrictive and destroys the purpose of the service. On the other hand, there would seem to be a strong case for allowing third parties to cancel calls transferred to them in order to mitigate possible draw drawbacks of the service (transferring a wrong number, for example).

This provision is vital to the liberalization of the market in this equipment.

It should also cover terminals such as answering machines with remote access, which are very badly protected at the moment. In particular, there are often several different secret codes for one machine. Article 15 should specify that answering machines with remote access should be effectively protected against unauthorized access.

There are grounds for wondering whether the provisions mentioned above regarding the identification of the caller and the confidentiality of correspondence do not in fact provide greater protection than the provisions of Article 16. If this is so, Article 16 would be dangerous or meaningless.

The Committee also thinks that there should be more sectoral specifications for these services.

The aim of these provisions is to use the public list of persons not wishing to receive unsolicited calls as a means of protecting subscribers. The Committee feels that this approach is inappropriate.

All calls—by whatever form of telecommunications—not wanted by the addressee constitute an invasion of his/her privacy. Appropriate means of prevention—not necessarily involving the operators of telecommunications networks—must be sought. In particular, suppliers of services using automatic calling machines with prerecorded messages should obtain the written consent of the persons concerned.

4. Proposal for a Council Decision in the field of information security

4.1. General and specific comments

4.1.1. The Committee endorses the need for coordinated action between Community-level projects on information and telecommunications technologies.

4.1.2. The Committee also endorses the need to promote products which better meet the needs of the business sector (such as Economic Development Institute (EDI)) and other non-governmental public and private sectors (administrative, medical, etc.) where data also need to be protected.

4.1.3. The Committee recognizes that security extends beyond the processing of personal data and the main security-related aspects of data protection (confidentiality, authentication). Overall vulnerability, availability, and other factors are also relevant.

4.1.4. The Committee notes that Member States retain ultimate control of the encryption services used by non-governmental sectors (private and public purely administrative or commercial sectors). Such issues as authentication, integrity and confidentiality cannot be resolved, when data are transmitted via telecommunications networks, without recourse to encryption techniques.

4.1.5. The Committee calls for the establishment of a committee and work plan. The draft Decision is imprecise as to the tasks, powers and working methods of the committee mentioned in Article 6. In particular, there should be no link between the procedures laid down by the general Directive and those contained in the draft Decision.

4.1.6. The Committee trusts that the first duty of this committee will be to assess needs, and that, after consulting the data protection authorities, it will draw up the necessary work plan in the near future.

5. Conclusions

5.1. The Committee is pleased that the Commission has taken account of the concern it has voiced on a number of occasions about the failure to protect personal data in plans for telematic networks, particularly those linking administrations. Nonetheless, it trusts that the definitive texts will be clearer and more consistent,
to ensure that the exercise of the rights established therein is practical, clear and homogeneous in all Member States.

5.2. The Committee draws the Commission's attention to four key principles which should underpin the Directive.

5.2.1. Protection must be provided against all processing of personal data, with a guarantee that this protection is strictly respected by all (States, institutions, public and private companies and organizations, etc.).

5.2.2. Once this has been established, telematic exchanges of data (using both present and future systems) must be permitted and developed, as they are vital to a dynamic Community (in trade, industrial, technical, social, cultural and other terms).

5.2.3. Materials and programmes used to this end must provide a technical guarantee of the above requirements at competitive prices.

5.2.4. Guarantees of data protection, developments in materials and programmes, and the technical means used to this end, must be the same for everyone throughout the Community.


5.3. The Council must immediately provide all Member States to take the necessary legislative measures to implement the principles of Council of Europe Convention 108.

5.4. The Committee is insistent on the following points:

5.4.1. The processing of personal data by the public sector should be explicitly subject to prior examination by the independent public authorities set up to ensure data protection.

5.4.2. The obligations to notify or carry out other preliminary investigations must be relevant and equivalent in all Member States.

5.5. The Committee considers that an independent European authority, along the lines of the national authorities, should be responsible for monitoring the implementation of the principles of the Directive in certain sectors or categories of personal data processing. This authority should also be responsible for follow-up and the formulation of security requirements and requirements for transfer to third countries.

5.6. The authority, to be attached to the EC Commission, should be made up of Member States' data protection ombudsmen.

5.7. When necessary, the authority should be able to bring matters before the Council of Ministers and should submit an annual report to the European Parliament and the Economic and Social Committee.

The Chairman
of the Economic and Social Committee
François STAEDELIN