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 contrary to the provisions of domestic law giving effect to the basic principles set out in Articles 5 and 6 of Convention 108,

— to have a remedy if a request for confirmation or, 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.

[1] OJ No C 277, 5. 11. 1990, p. 3-12.

1.3.1. Accordingly, any person who orders or carries out 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.

1.4. These principles are mainly covered by Articles 16, 17 and 18 of the proposed general Directive (SYN 287).

1.4.1. 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.

1.4.2. 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 drafting of sectoral provisions.

1.5. 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 gives 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.

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

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

1.5.3. 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. Proposal for a Council Directive concerning the protection of individuals in relation to the processing of personal data—SYN 287

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 [1] and a precise definition of the personal data which must be protected [2]. 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 files' 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 (integrated 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 'file', 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)(c), 8(2) 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 clearer than the explanation given 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 their 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.

File

2.2.2.4. The Committee feels that manual files should also be covered; this should include collections 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.

[1] OJ No C 41, 18. 2. 1991, p. 6.
[2] OJ No C 41, 18. 2. 1991, p. 12.

Processing

2.2.2.6. The definition of processing should include data collection.

Independent public authority

2.2.2.7. The Committee considers that the independent nature of the relevant national authority is a useful addition *vis-à-vis* Convention 108.

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

Distinction between the public and private sectors

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

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

Communication

2.2.2.11. In order to clarify the implementing conditions of certain provisions of the Directive the term 'communication' should also be defined.

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

2.2.3. Article 3 — Scope

2.2.3.1. The Committee endorses the proposed exemptions.

2.2.3.2. It considers that processing by trade organizations and charitable organizations should also be exempt.

2.2.3.3. Notwithstanding the proposed exemption conditions, the Committee considers that the general principles of Convention 108 should continue to apply to such processing to guard against improper use.

2.2.4. Article 4 — Law applicable

2.2.4.1. The exemptions for 'sporadic' use or a file being 'moved temporarily' could be dangerous. They would allow anyone to conduct highly sensitive but temporary operations without being subject to protection measures.

2.2.4.2. 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).

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

2.2.5.1. 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.

2.2.5.2. 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.

2.2.5.3. 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.

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

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

2.2.5.6. 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.

2.2.5.7. Such controls should only be exercised selectively.

2.2.5.8. 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 the 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 sould be subject to the agreement of the patient and should 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 only 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 of the issuers of dishonoured bills of exchange, cheques, etc.) should be subject to both *a priori* and *a posteriori* control.

2.2.11. Articles 12, 13 and 14

2.2.11.1. These Articles list the rights of data subjects and are based on the provisions of Convention 108, with 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 (banning of decisions taken solely on the basis of the automatic processing of Personal data defining the subject's personality profile) which is not used elsewhere.

2.2.11.2. However, some of these rights deserve to be interlinked and more flexibly applied in the light of their relevance to private data processing, in order to avoid the problems mentioned in 2.2.9.

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

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

2.2.12. Article 15

2.2.12.1. Possible reasons for granting exceptions to 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 and the rights and freedoms of others'. The latter covers economic freedoms (business and commercial secrecy).

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

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

2.2.13. Article 16

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

2.2.14. Article 17 — special categories of data

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

2.2.15. Article 18

2.2.15.1. 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.

2.2.15.2. 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.

2.2.15.3. 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).

2.2.16. Article 19

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

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

2.2.17. Article 20

2.2.17.1. 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 feels that the proposed procedure is inappropriate.

2.2.20. Article 26

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

2.2.20.2. In the light of the comments in 2.2.5 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 adaptation 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 seem 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

certain sectors, as regards security and transfers to third countries.

2.2.22.2. Article 30 provides for the establishment of an advisory committee made up of representatives of the Member States and (again) chaired by a Commission representative. The respective tasks of this committee and of the working party are not clearly distinguished.

2.2.22.3. The Committee's comments on control of the public sector, security, codes of ethics, and transfers to third countries would suggest that some other type of balance of powers is necessary.

2.2.22.4. In particular, the need to safeguard basic rights means that the authority in charge must be independent.

3. **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 (SYN 288)**

3.1. *General comments*

3.1.1. The proposal provides a good basis on which to work; it is clearly based to a large extent on the work carried out in this field by data protection officials.

3.1.2. The approach is the right one because:

— it adds principles which are specific to this sector to the principles laid down in the general Directive,

— in application of these principles, it specifies concrete measures for providing effective and equivalent protection service-by-service and network-by-network or whenever necessary. Technical aspects are also taken into account,

— in the interests of consistency with the general Directive (SYN 287), the Directive should only deal with (a) international telecommunications services so as to standardize their operation in all Member States, and (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.

3.1.3. For the Articles dealing with procedural matters (Article 22 et seq.) the Committee refers back to its comments on the general Directive.

3.1.4. The definition of the term 'telecommunications organization' (Article 3) refers to a 'public telecommunications network'.

3.1.5. In the Committee's view, this should be amended to read 'telecommunications network open to the public', to distinguish it from internal private networks.

3.2. *Specific comments*

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 ombudsmen, 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—provisions which may seem arbitrary.

3.2.2. Article 4(2) on the electronic profiles of subscribers: the outright ban is an extreme solution. Tele-

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 organizations should widely publicize this innovation, and retain their policy of anonymous payment in public booths.

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 a subscriber and his/her exchange, which may be either digital or analogue. Idenfication 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. Subcribers who accept identification must retain the right to decide otherwise at short notice.

3.2.5.4. At all events, under the Commission's proposal, the subscriber called will always be able to refuse 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 why this derogation from the rule eliminating the 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 problems in principle. However, the feasibility of obtaining the con-

sent of the subscriber to whom the call is to be forwarded is questionable.

3.2.6.2. 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 (transfer to a wrong number, for example).

3.2.7. Article 15 — Telephone terminals with loudspeakers or recording equipment

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

3.2.7.2. 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.

3.2.8. Article 16 — videotex services

3.2.8.1. 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.

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

3.2.9. Article 17 — unsolicited calls

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

3.2.9.2. All calls—by whatever form of telecommunications—not wanted by the addressee constitute an invasion of his/her privacy. Appropriate means of protection—not necessarily involving the operators of telecommunications networks—must be sought. In particular, the suppliers of services using automatic calling machines with prerecorded messages should obtain the prior approval 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, authentification). 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 authentification, 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 prevail on all Member States to take the necessary legislative steps to implement the principles of Council of Europe Convention 108.

5.4. The Committee is insistent on the following two 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 supervise 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 general 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.

Done at Brussels, 24 April 1991.

The Chairman

of the Economic and Social Committee

François STAEDELIN