

EXPLANATORY MEMORANDUM

to Recommendation No. R (2002) 9 of the Committee of Ministers to member states on the protection of personal data collected and processed for insurance purposes

(Adopted by the Committee of Ministers on 18 September 2002 at the 808th meeting of the Ministers' Deputies)

Foreword

The Council of Europe is a political organisation that was set up on 5 May 1949 by ten European states in order to achieve a greater unity between its members.¹

The Organisation's main aims are to promote democracy, human rights and the rule of law, as well as to seek common solutions to its member states' political, social, cultural and legal problems. Since 1989, it has taken in most of the central and east European countries and is helping them in their efforts to implement and consolidate their political, legislative and administrative reforms.

The Council of Europe's action so far has resulted in the adoption of over 178 European conventions and agreements, which form the basis of a "common legal area" in Europe. Many of the Committee of Ministers' recommendations propose principles for action by the national governments.

The Council of Europe has its permanent headquarters in Strasbourg (France). The Organisation's Statute provides for two consultative bodies, namely the Committee of Ministers, made up of the ministers of foreign affairs of the forty-four member states, and the Parliamentary Assembly, comprising delegations from the forty-four national parliaments. The Congress of Local and Regional Authorities of Europe represents territorial collectivities in the member states.

The European Court of Human Rights is the judicial body responsible for adjudicating applications submitted against specific states by individuals, associations or other contracting states for violations of the European Convention on Human Rights.

The Council of Europe's role and activities in the data protection field

One of the Council of Europe's first conventions, which is also one of the most important - it is provided for in Article 1 of the Organisation's Statute - is the Convention for the Protection of Human Rights and Fundamental Freedoms, opened for signature in 1950. This Convention characterises the European specificity with regard to human rights, which relates in particular to the fact that states which have ratified the Convention and have recognised the obligatory nature of the Court's jurisdiction must abide by the judgments of the European Court of Human Rights.

Several provisions of this Convention are relevant to "the protection of individuals with regard to automatic processing of personal data", particularly Articles 8 and 10. Conversely, data protection is geared to clarifying the scope of certain provisions of the Convention and their interrelations.

According to Article 8 of the Convention, "everyone has the right to respect for his private and family life, his home and his correspondence". There shall be no interference by a public authority with the exercise of this right except where such interference is in accordance with the law and is necessary in a democratic society to defend certain legitimate goals, which are listed exhaustively. However, Article 10 of the Convention also confirms the fundamental right to freedom of

expression. This right explicitly includes the freedom "to receive and impart information and ideas without interference by public authority and regardless of frontiers".

In the logic of the Convention, Articles 8 and 10 are complementary rather than contradictory. In practice, though, each of these rights sometimes restricts the enjoyment of the other. The organs of the European Convention on Human Rights have, therefore, used their case law to determine the limits on the exercise of each of these rights. In particular, they specify the extent to which the public authorities are entitled to interfere with rights recognised by the Convention or are encouraged to accompany certain sectors with legal safeguards. The Court, for instance, ruled that data protection was a fundamental element of the protection afforded to the right to respect for privacy.² These decisions are therefore highly relevant to the Council of Europe's activities in the data protection field. Furthermore, they have been, and still are, a major source of criteria on which the governments can base their national regulations. Nevertheless, it has become clear over the years since the adoption of the European Convention on Human Rights that, to be effective, the legal protection of privacy must be developed along more specific and systematic lines.

In the early 1960s, the rapid progress made in the field of electronic data processing and the advent of the first computers enabled government departments and large firms to establish large databases and improve and increase the collection, processing and linking of personal data. While these developments offered great advantages from the standpoints of efficiency and productivity, they also led to a failure to provide sufficient guarantees in the electronic recording of data. In response to this phenomenon, at the initiative of the Parliamentary Assembly, the Council of Europe decided to establish a body of principles and special rules to prevent the unfair collection and processing of personal data in both the public and the private sectors.

The first steps were taken in 1973 and 1974 with the adoption of Resolutions (73) 22 and 74 (29) setting out the principles governing the protection of the privacy of individuals vis-à-vis electronic databanks in the private and public sectors. The aim was to encourage the drafting of national legislation based on these principles. However, when these resolutions were being drawn up it was acknowledged that, to be effective, national rules and international co-operation governing the general protection of personal data should be supplemented by internationally binding standards. The same suggestion was made at the 1972 European Conference of Ministers of Justice.

The result was the opening for signature on 28 January 1981 of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS No. 108), or Convention 108³, which was the first legally binding international instrument in the data protection field. Under this Convention, the parties are required to take the necessary steps in their domestic legislation to apply the principles it lays down in order to ensure respect in their territory for the fundamental human rights of all individuals with regard to the processing of personal data. The principles are particularly concerned with data quality, namely:

- data must be obtained and automatically processed fairly and lawfully;
- data must be recorded for specified and legitimate purposes;
- data must not be used in a way incompatible with those purposes;
- data must be stored only for as long as is required for these purposes;
- data must be recorded in an appropriate, relevant and non-excessive (proportional) manner vis-à-vis the said purposes; and
- data must be accurate.

They also concern:

- prohibiting automatic processing of sensitive data (political opinions, religious beliefs, race, criminal convictions, medical data, etc.), unless appropriate guarantees are provided;
- informing data subjects;
- rights of access and rectification.

Convention 108 also provides for the free flow of personal data between parties to the convention. This free flow shall not be restricted for the purposes of data protection. However, parties can derogate from these provisions:

- where another party does not provide "equivalent" protection; or
- where a transfer is destined for a country which is not party to Convention 108.

The additional protocol to Convention 108, adopted on 23 May 2001, requires parties to set up one or more independent supervisory authorities, and requires them to prohibit, in principle, transborder flows of data to countries or organisations which do not provide an appropriate level of protection.

Convention 108 establishes a Consultative Committee, made up of representatives of the parties to the convention, which interprets its provisions and seeks to facilitate and improve its application. One of the committee's initiatives has been to examine how far the use of contractual clauses could facilitate transfrontier data flows between parties to the Convention and non-contracting states, and it has developed, in conjunction with the European Commission and the International Chamber of Commerce, a model set of contractual clauses.

Article 4 of Convention 108 stipulates that parties must adopt measures in their domestic legal systems to give effect to the data protection principles set out in Convention 108 before they can become contracting parties, and so far twenty-eight member states⁴ have ratified it. Others⁵ have signed the Convention 108 and some of them have enacted data protection legislation and are preparing for ratification. Several member states of the Council of Europe list data protection among the fundamental rights of their constitution. Article 23 of Convention 108 also authorises Council of Europe non-member states to accede to the Convention. On 15 June 1999 the Ministers' Deputies of the Council of Europe adopted an amendment to Convention 108 permitting the accession of the European Communities. This amendment will come into force thirty days after agreement by all parties.

Since the adoption of Convention 108 in 1981, society has become so computerised as to make the use of personal computers and electronic networks an everyday occurrence, so that any individual or organisation can now undertake "automated data processing". Over the intervening period, social and economic developments have been reflected in ever more complex forms of organisation, management and production based on powerful processing systems. As a result, individuals are undoubtedly becoming active participants in the information society, which in turn poses an increasing threat to their privacy through the medium of information systems run by private and public sector bodies such as banks, credit institutions, social security, insurance companies, the police and medical services.

This trend represents a considerable challenge for data protection. The adoption by the Committee of Ministers, on 7 May 1999, of the Declaration on a European Policy on New Information Technologies, which mentions data protection, reflects the importance of seeking joint solutions to the problems arising out of the development of these technologies.

An ever-increasing number of new problems and practical questions are being submitted to the national authorities responsible for data protection, or, in most countries, data protection commissioners.⁶ These authorities have become an integral part of the monitoring systems in democratic societies. They are required to interpret their domestic law in accordance with the principles of Convention 108 and apply them to new problems and questions. The development of case law in the data protection field helps provide specific solutions to specific problems, which arise in different forms depending on the sector under consideration.

The general principles of data protection must be more clearly specified in practice. The provisions of Convention 108 and the requisite general legislation on data protection at domestic law level

cannot deal precisely with all the situations arising in the different sectors where personal data are collected and processed. Specific rules are needed for each sector: health, social security, insurance, banking, employment, the police, telecommunications, direct marketing and so on. In all of these sectors data must be collected and processed in accordance with the fundamental principles of Convention 108 but the ways of doing so may differ. The conditions may be more flexible in some sectors than in others and self-regulation more developed in one profession than in another.

Drawing on Convention 108, the Council of Europe has adopted several sectoral recommendations. These Committee of Ministers recommendations are intended for the governments of all the Council of Europe member states. Although they are not legally binding they do constitute reference standards and invitations to consider, in good faith, the possibility of drafting and applying domestic legislation in accordance with an agreed international interpretation of the principles laid down in the Convention and the recommendation.

In 1976, the Committee of Ministers set up a Committee of Experts on Data Protection, which subsequently became the Project Group on Data Protection (CJ-PD), to draw up these different recommendations. The committee comprises experts representing each of the forty-four member states with data protection responsibilities in their respective countries. In order to deal with specific issues the experts are sometimes accompanied by specialists in the area concerned. Reflecting traditional Council of Europe practice, observers from employers' and employees' organisations and non-governmental organisations working in the relevant field are also invited to attend such intergovernmental meetings. The European Commission also takes part in drawing up these recommendations, particularly in areas for which it has responsibility, on the basis of Directive 95/46/EC of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

Over the years the Project Group has not only produced a series of recommendations⁷ but has also published studies on specific topics in the data protection field.⁸

Introduction

A. The challenges

1. The growing computerisation of activities and constant technological developments inevitably have an impact on contemporary society and interpersonal relations. The instant exchange and processing of large quantities of information are matters of interest for both individuals and commercial undertakings, including the insurance industry.
2. At the same time, close attention must be paid to the risks that such progress poses for human rights and fundamental freedoms, particularly the right to respect for privacy.
3. Insurance companies attach great importance to respect for privacy and security. These concerns are shared by their clients and potential clients, in other words those affected by any potential processing of their data, for whom the confidentiality of their dealings is a key consideration.
4. This Recommendation is intended to strike a balance between the interests of insurance companies and normal business operations on the one hand, and the protection of privacy on the other hand.
5. Insurance companies need to collect and process data to ensure that they have correctly identified and set the right charges for the risks they are insuring. A proper knowledge of the risks enables them to operate in accordance with their customers' needs. A lack of information would inevitably impede their activities. Data processing also plays a key role in combating fraud: insurance companies need to exchange and transfer information to counter fraud, which is prejudicial to other insured parties.

6. Insurers are required to deal with personal data, particularly medical data, for example in the life and sickness insurance fields.
7. Collecting and processing personal data for insurance purposes requires supervision to ensure that the data are not used unfairly or illegally. Such supervision must also be applied to international transfers to countries lacking a satisfactory level of protection. In particular, it is important to avoid the risk that data collected and processed for specific legitimate purposes will subsequently be used for purposes other than the original ones. Special care must be taken to prevent any processing resulting in discrimination between insured parties or categories of insured parties.
8. The specific principles for the insurance industry set out in this Recommendation are an attempt to respond to all these concerns.
9. The Recommendation applies to all commercial undertakings concerned with insurance, whether insurance companies or brokers, but does not apply to state social security schemes, unless individual governments decide to extend the scope of their domestic law implementing the Recommendation to make it applicable to their social security schemes.

B. Characteristics of the insurance industry

10. Insurance is a means of limiting the negative consequences of uncertainty. Thus, through an insurance company, individuals or businesses share risks on a mutual basis so as, if not to eliminate uncertainty, at least to minimise its negative effects. The basic concept of insurance is both intensely individual - as the persons insured seek to protect themselves against the negative impact of this or that unfortunate eventuality - and intensely collective, because by protecting him or herself each individual also protects the rest. By reducing the negative consequences of hazards to physical resources (through general insurance) and to human resources (through life insurance), insurance becomes a powerful mechanism for generating security, fostering the pursuit and development of economic and social activities and the proper functioning of agreements of all types, and helping to reduce the disparities that inevitably arise if everything is left to chance.
11. Insurance is an organised activity involving both certain specific elements and certain technical rules. According to one classic definition, there are four key elements:
 - a. the risk: an uncertain future event beyond the control of the insured person, or an event that is certain to occur but at an unknown date;
 - b. the premium: a payment by the insured person to the insurer in return for a guarantee;
 - c. the benefit payable by the insurer: should the risk materialise, the insurer will pay out a benefit;
 - d. a system of compensation through a mutual fund: all subscribers to the fund pay their premiums without knowing whether they or someone else will benefit from them, but aware that it is their payments, along with those of the other subscribers, that enable the insurer to compensate persons who suffer loss. Collectively, the persons insured against a common risk and paying premiums together as a means of coping with its consequences constitute a mutual fund. The insurer thus organises a system of solidarity between the insured persons against the occurrence of a particular event.
12. The insurance industry uses statistical methods to calculate risk. These are based chiefly on the law of large numbers (the results of studies covering a very large number of cases indicate with sufficient accuracy the probability that an event will occur) and on loss data, which are indispensable to insurers. By using such methods they can calculate the frequency of risk occurrence and the average cost of claims for loss.

13. The nature of the insurer's activity in managing the body of premiums that constitutes the fund entails setting aside considerable sums in the form of provisions against future commitments. These provisions, which are the subject of strict regulations designed to protect insured persons, are a major source of investment in national economies.

C. Changes in the rules governing data protection

14. Parliaments, and in some countries the insurance industry itself, have drawn up data protection standards or established safeguards in the insurance field. Several countries have introduced codes of ethics. Specific sectoral rules have sometimes been established to control or prohibit the industry's collection and use of certain data such as genetic data, which may reveal individuals' or families' hereditary characteristics.
15. Data-protection legislation is aimed at guaranteeing fundamental human rights, particularly privacy. The insurance business must conform to confidentiality rules which partly pursue similar aims, and the rules or practices are therefore essential complements to national legislation, because insurance activities must not be allowed to proceed without an appropriate legal framework. Self-regulation and the use of appropriate techniques complement this framework.

D. Chronology of the Recommendation

16. In November 1990, the Project Group on Data Protection decided to examine the data protection problems posed by the collection and processing of personal data in the insurance industry, with a view to preparing an appropriate legal instrument.
17. Working Party 14 was established for that purpose. It was chaired by Dr J. A. Cannataci (Malta) and included experts from Germany, Malta, Norway, Spain, Sweden, Switzerland and the United Kingdom. It met six times between February 1994 and October 1996. The meetings were attended by experts in respect of Albania, Austria, Belarus, Belgium, Bulgaria, Canada, Croatia, Hungary, Luxembourg, the Netherlands, Russia and "the former Yugoslav Republic of Macedonia", as well as representatives from the European Commission, the International Chamber of Commerce, the European Insurance Committee and the International Association of Insurance and Reinsurance Intermediaries.
18. The European Commission helped to draw up the Recommendation within its area of responsibility and on the basis, in particular, of the provisions of Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.
19. The draft Recommendation on the protection of personal data collected and processed for insurance purposes was approved by the Project Group on Data Protection at its 37th meeting, from 12 to 15 October 1999, and by the European Committee on Legal Co-operation on 31 May 2001.
20. On 18 September 2002, the Committee of Ministers adopted Recommendation No R (2002) 9 on the protection of personal data collected and processed for insurance purposes and authorised the publication of this explanatory memorandum.

Comments on the provisions of the Recommendation

Preamble

21. The preamble sets out the Committee of Ministers' reasons for addressing the Recommendation to the member states' governments.

- a. Among these considerations, the Committee of Ministers refers to the need, in the insurance field, to promote and guarantee protection of personal data, particularly sensitive data as provided for in Article 6 of Convention 108.
- b. It also acknowledges the need for the automated processing of large quantities of personal data, to facilitate rational and economic management of insurance in a highly competitive industry and to fight against fraud.
- c. The Committee of Ministers notes that responsibility for supplying insurance in the various branches of the insurance sector and the different categories of contract is not confined to insurance companies. Insurance intermediaries play a key role in this area. Lastly, the state intervenes also to regulate the insurance sector. Moreover, authorities or bodies exercising public functions themselves sometimes provide insurance.
- d. The Committee of Ministers refers to the many situations in which taking out insurance is quite normal or has become essential, either because of a legal obligation, as in the case of motor insurance, or because of a generally accepted practice. As a result, individuals are required to supply a considerable amount of information pertaining to their private lives, and in particular sensitive data, which is then extensively processed for different insurance purposes.
- e. It recognises, in accordance with Article 5 of Convention 108, the importance of the quality of data collected and processed in the insurance field, in particular, especially their relevance, integrity, availability and confidentiality, since this is an inherent aspect of any relationship of confidence between insurers and insured persons, as it is in the case of banks and other financial institutions.
- f. It defines the Recommendation's objective as the establishment of appropriate procedures for ensuring that personal data for insurance purposes are collected and processed in a manner compatible with individuals' fundamental rights and freedoms and that a proper balance is struck between the free circulation of information and respect for privacy. Such a body of regulations is made necessary by the increasing mobility of individuals and the globalisation of markets and commercial activities, which in turn necessitate exchanges of information across frontiers and an equivalent level of protection in all Council of Europe member states.

The body of the Recommendation

- 22. The Committee of Ministers recommends firstly that governments of member states take measures to ensure that the principles contained in the appendix are reflected in their law and practice. The wording of this Recommendation is also aimed at member states that are not yet parties to Convention 108 and have, therefore, not yet taken all necessary steps in their domestic law to apply the basic principles of data protection.
- 23. Secondly, governments are encouraged to circulate widely the content of the appendix to the Recommendation to national authorities with data protection responsibilities as well as to all those in the industry required to collect and process personal data for insurance purposes or ensure that such data are protected.
- 24. Thirdly, governments are invited, where necessary, to promote legislation in the insurance field and encourage the drafting of codes of ethics based on the principles in this Recommendation.

Appendix to the recommendation

1. Definitions

25. **Chapter 1** lays down definitions for some of the Recommendation's central concepts. The expressions "domestic law", "law", "provided for by domestic law" and "authorised by domestic law" were defined in Recommendation No. R (97) 18 concerning the protection of personal data collected and processed for statistical purposes (paragraph 50 of the explanatory memorandum), in accordance with the case law of the European Court of Human Rights.
26. **Personal data:** the definition is compatible with that used in Convention 108, as interpreted in its explanatory memorandum. It has already been used in many sector-specific recommendations adopted by the Committee of Ministers in the data protection field.
- a. **Person:** the definition refers to an individual. However, in the case of Parties which extend the application of Convention 108 to legal persons (in accordance with Article 3, paragraph 2.b of Convention 108 or Principle 2.4 of the Recommendation), the latter are also included in the scope of the definition. Moreover, information relating to individuals may concern entities, for example one-person businesses, while still constituting personal data (relating to the owner for example). In such cases, it comes within the scope of the Recommendation.
 - b. **Identifiable person:** persons are "identifiable" when they can be identified through the processing or cross-checking of their personal data, particularly through reference numbers or one or more specific factors relating to their physical, physiological, psychological, economic, cultural or social identity. Persons are not identifiable if identification requires unreasonable activities, in other words excessively complicated, long and costly operations. These conditions are judged, *inter alia*, in the light of the technical resources available for identifying the relevant data and thereby penetrating their anonymity. Given the rapid progress in data processing techniques and methods, therefore, what would today be considered an unreasonable amount of cost, time and effort to identify a person might not be so in the future. However, the current wording is sufficiently flexible to take account of such developments.
27. **Sensitive data:** the definition is based, in particular, on the minimum list in Article 6 of Convention 108. It also includes criminal proceedings, on the model of Article 8 of Directive 95/46/EC. In accordance with Article 11 of Convention 108, other categories of personal data (such as data on trade union membership) may be defined as sensitive by domestic law. For the definition of medical data, reference should be made to Recommendation No. R (97) 5 on the protection of medical data, also as far as genetic data are concerned (see its explanatory memorandum, paragraphs 41-58).
28. **Insurance purposes:** in the absence of a generally accepted definition of insurance at the international level the definition of insurance purposes is the broadest possible. This definition stresses the purposes of processing rather than arbitrarily delimiting the various sectors concerned. The definition covers all data collecting and processing operations inherent in the insurance process, linked, for example, to covering a risk or preparing, concluding, implementing or terminating insurance contracts or policies. The definition covers all insurance operations, regardless of the type of agency undertaking such operations, whether insurance companies, intermediaries or public bodies. It also covers retirement plans, but on the other hand excludes gambling. This definition also includes social security for those states which desire to use the option of extending the scope of domestic law implementing this Recommendation to social security, in accordance with Principle 2.5.
- a. Insurance "cover" is defined as an operation under which an insurer is required, in return for remuneration in the form of a premium, to provide the insured party or a third person with a benefit in the event of occurrence of a given risk. Such coverage may be based on a contract,

a policy or any other form of establishment of a legal obligation, such as legal systems of protection against risks of illness, invalidity and old age applied, for instance, in respect of commercial or industrial employees. It may, therefore, be drawn up on the initiative of persons wishing to take out insurance, or may result from a legal provision. Indeed, in the majority of cases such insurance cover will be accompanied by a contract, whether or not the insurance is obligatory. But in certain countries, insurance cover, for example, for properties may be tantamount to an administrative requirement.

- b.* The "risk" specific to insurance activity depends on the determination, generally jointly by the insurer and his client, of a contingency, damage or any other event more or less certain or likely to happen in the future.
 - c.* Moreover, the expression "any operation" covers the collection and the processing of personal data by the insurer for the coverage of a risk. It also covers intermediary insurance operations. Intermediaries, such as brokers, play a key role in the insurance sector, in particular in preparing contracts and reinsurance. Brokers set out to find the best cover for their clients with the lowest possible premiums. To achieve this, they send certain personal data to a number of insurance companies in order to obtain offers. The expression also covers operations carried out by experts in their activities linked to insurance.
 - d.* According to Article 5 of Convention 108, personal data must only be processed for specified purposes. They must not be used in a manner incompatible with these purposes. Therefore, for the purposes of this Recommendation it is important to determine the "insurance purposes". This is why these purposes, and the purposes with which they might be compatible, are specified in particular in Principle 4.4 or in relation to Principles 4.8, 8.1 and 13.1 of the Recommendation. The general purpose of insurance should therefore be considered in the light of the definitions related to the coverage of a risk and the particular purposes specified in this Recommendation.
- 29. Processing: the definition encompasses all automated operations required for the insurance process, with the exception of data collection when this is not followed by automated processing. The scope of these operations is dealt with in Chapter 2 of the Recommendation. The choice of applying this Recommendation to non-automated processing lies with the member states.
- 30. Communication: the term covers all actions allowing the data to be made available to a third party, including transmission, dissemination and interconnection. The data may be made available actively - by replying to an individual request by the third party - or passively - by granting the third party on-line access to personal data.
- 31. **Controller:** the term refers to the concept of "controller of the file" as set out in Article 2 of Convention 108. However, the term "file" does not take sufficient account of technological developments in the processing of personal data. As with previous recommendations, this Recommendation defines the concept of "controller" as applying to any individual or body responsible for determining the purposes and means of personal data collection and processing for insurance purposes. This concept is analogous to that established in Article 2.d, Directive 95/46/EC. It is incumbent on each member state to ask any controller who is not based within its national territory to appoint a representative to guarantee compliance with the obligations set out in the Recommendation.
 - a.* The definition covers insurers, organisations or persons providing insurance, as well as intermediaries. Brokers, independent agents and also, where necessary, experts or financial institutions should, in principle, be considered as controllers and not as processors to the extent that they collect and process personal data, even before the conclusion of a contract.

Responsibility for compliance with data protection principles lies with the controller, with the exception of specific security obligations for any processor involved.

- b. The reference to public authority is included in the definition because, for instance, some types of insurance for industrial injuries are provided by public authorities. Similarly, public bodies are generally responsible for credit guarantees and other aids to exporters, especially *vis-à-vis* insurance cover for political risks.

32. Processors: this term takes account of the specific activities of persons specifically appointed to carry out part or all of processing on behalf of and in the name of the controller. The processor's responsibility differs from that of the controller from the point of view of data protection, in conformity with Chapter 7 of the Recommendation. The concept of processor is analogous to that laid down in Article 2.e of Directive 95/46/EC.

2. Scope

33. Principle 2.1 defines the scope of the Recommendation as "personal data collected and processed for insurance purposes". Social security is explicitly excluded from the scope of the Recommendation in view of the different rules applicable to private insurance, on one hand, and social security, on the other hand, under the domestic law and practice of most states and in international law. However, to the extent that domestic law and practice in some states make it possible to assimilate social security to insurance from the data protection regulation point of view, Principle 2.5 provides for the possibility of states extending the scope of this Recommendation to social security, given the wide definition adopted of "insurance purposes". The Recommendation also covers, *inter alia*, insurance operations by intermediaries, in which brokers or agents deal with personal data. Strictly speaking, brokers do not conclude insurance contracts; if they do, insurance companies always reserve a "right of acceptance". While brokers are deemed to act on behalf of insured persons, agents generally act on behalf of insurers.

- a. In the insurance field, data are often collected manually through the completion of forms. Sometimes these manual files contain sensitive data. The Recommendation therefore applies to any personal data collected for insurance purposes, whether this is done by automated means or by manual means with a view to further automated processing.
- b. The term processing, as defined in Chapter 1, covers a wide range of operations. The Recommendation therefore applies to all these forms of automated processing of personal data.

34. Principle 2.2 encourages states "to extend the application of this Recommendation to non-automated processing of personal data for insurance purposes". Indeed, under Article 3, paragraph 2.c of Convention 108, parties can extend its scope to personal data files which are not processed automatically.

- a. In practice, immediately after they have been collected, data are often processed partly automatically and partly manually. In certain cases, personal data are recorded or stored manually.
- b. The growing computerisation of activities is, however, tending to reduce the number and the importance of manual files.
- c. Data protection legislation in some member states does not apply to manual files. However, some other countries have already extended the scope of their legislation to non-automated data processing. Directive 95/46/EC in fact applies to "structured" manual files.

- d.* States are free to decide how and how far this extension should apply. The Recommendation encourages this extension, thus covering files which may sometimes contain sensitive data. Finally, states may provide for a transitional period for the extension of the scope of the recommendation to data processed manually for insurance purposes.
35. According to Principle 2.3, under no circumstances should data be processed manually in order to avoid applying the principles set forth in the Recommendation. This provision is intended to prevent practices designed to get round the data protection principles where national legislation does not apply to non-automated processing.
36. Principle 2.4 authorises an optional extension of the Recommendation's scope to the protection of data relating to legal persons and other organisations collected and processed for insurance purposes. The aim is to offer effective protection to individuals' privacy, while at the same time granting states the authority, provided for in Article 3.2.b of Convention 108, to include not only natural persons, but also groups of persons, associations, foundations, companies, corporations and any other bodies consisting directly or indirectly of individuals, whether or not such bodies possess legal personality.
37. Personal data collected and processed for social security purposes are already covered by Recommendation No. R (86) 1. The different member states have a wide variety of social security systems, and it was deemed appropriate to confine the scope of the Recommendation to insurance activities and leave it to the governments to decide whether or not to apply its provisions to the social security field. Principle 2.5 therefore, grants states that so wish the additional authority to extend the Recommendation's scope to the collection and processing of personal data used for social security purposes. When the extension option is used, in principle the collection and processing of data used for social security purposes is governed by Recommendation No. R (86) 1 on the protection of personal data used for social security purposes, in so far as the present Recommendation is not applicable. This means that there will be no legal uncertainty in cases where insurers provide social and private insurance or in cases of transborder data flows between states with different systems.
38. This option is justified by the fact that some member states consider social security as a branch of insurance, particularly because some of the management of social insurance is entrusted to private or semi-public bodies that also provide private insurance benefits. This applies to sickness insurance, one part of which comes under compulsory social insurance and another part under complementary private insurance. In such cases it might be justified not to make personal data processing subject to different legal regulations. This option would also take account of the current economic trend towards privatisation of entire sectors of social security, which had traditionally been in the hands of public bodies. It caters for the difficulty of drawing a clear distinction between the public and private sectors, between insurance and social security: for instance, industrial accidents in some countries fall within the public domain, but the private sector issues the relevant contracts. In other countries, whole swathes of the industrial accident field are being transferred to the private sector. Similarly, in yet other countries health insurance is largely entrusted to private insurers. Lastly, this option respects those social security systems in member states that are governed by special legislation lying outside the usual rules of insurance and use a special financing system. In such cases, Recommendation No. R (86) 1 applies to the collection and processing of personal data used for social security purposes.

3. Respect for privacy

39. Principle 3.1 reiterates the purpose of Convention 108 as laid down in its first article, which is to ensure respect for all individuals' fundamental rights and freedoms, particularly their right to privacy, with regard to automated processing of their personal data.

40. Principle 3.2 stipulates that persons involved in insurance activities who have access to personal data must respect confidentiality in accordance with domestic law and practice, possibly complemented by codes of ethics approved by the industry.
41. The principle also makes it clear that medical data, in particular, can only be collected and processed by health professionals or persons subject to confidentiality requirements laid down in domestic law that are comparable or equally effective.

4. General conditions governing the collection and processing of insurance data

42. Principle 4.1 sets out certain basic data protection principles. The Recommendation explains that communication, as well as interconnection, form part of the definition of processing and that personal data can only be communicated in accordance with the provisions of the Recommendation, particularly Chapter 4. Chapter 8 specifically concerns the communication of personal data for other than insurance purposes.
- a.* In line with Article 5.a of Convention 108, the Recommendation reiterates the principles to the effect that personal data must be obtained and processed fairly and lawfully. The principle of fairness of collection and processing is covered, in particular, in Chapter 5 on information for the data subjects with a view to ensuring transparency of processing, but also concerns collection and processing methods. Lawfulness is dealt with in Principle 4.3.
 - b.* In accordance with article 5.b of Convention 108, the Recommendation also stipulates that personal data for insurance purposes can be collected and processed only for specified and legitimate insurance purposes. The purpose, which should be specific and explicit, is covered by Principle 4.4 where it concerns an insurance purpose or any purpose which is, in principle, compatible. Principles 4.8 (direct marketing), 8.1 (communication for purposes other than insurance) and 13.1 (storage) cover other purposes. Not all purposes of processing are legitimate in themselves, because even if carried out on a lawful basis, processing may, for instance, lead to discrimination between data subjects.
 - c.* The second paragraph of Principle 4.1 also illustrates the application of the proportionality and accuracy principles, which are based on Article 5.c and *d* of the Convention: the data processed must be adequate, relevant and not excessive in relation to the data controller's purposes at the time of collection and subsequently, and must be accurate; if necessary, they must also be updated. In the insurance field, as in others covered by specific recommendations, the proportionality principle implies that the collection and processing of personal data must be confined to personal data that are necessary for the relevant insurance purposes, having regard to the area of insurance concerned.
43. Principle 4.2 stipulates that personal data must in principle be collected from the data subject or his/her legal representative. In practice, data are not necessarily collected from the data subject, but from a third party, a fact which is taken into account in Principle 5.3 on information for data subjects. Data on the data subject may be collected from another person, if this is provided for by law (Principle 4.3) or where an intermediary is involved or in cases of reinsurance or attempts to detect fraud (for example, fraud to life insurance, false declaration to car insurance). When data are collected in such circumstances, the data subject must be informed under the conditions set out in the Recommendation.

Lawfulness

44. Article 5 of Convention 108 stipulates that personal data must be obtained lawfully. This means that the legality of the collection and processing of personal data for insurance purposes must be based on the law, on a contract, on the data subject's consent or on a legitimate interest pursued by the controller. These four conditions of lawfulness are alternatives.

45. Principle 4.3 is concerned with the application of the general conditions of lawfulness to the different types of personal data collection and processing for insurance purposes.
- a.* Sub-paragraph *a* is specifically concerned with situations in which the collection and processing of such personal data for insurance purposes are provided for in law. An obligation to supply information may then be imposed directly on data subjects, taking out a statutorily required insurance (for example, for property insurance in certain countries), but it can also be imposed indirectly on the controller where data are being collected pursuant to Principle 4.4.*h*. In this last case, an insurance company may be led to collect and process data itself, for example with a view to combating money laundering or organised crime. The communication of such data to the public authorities is governed by Chapter 8 of the Recommendation.
 - b.* According to sub-paragraph *b*, a contract can also be the legal basis for the collection and processing of personal data. The following factors are relevant:
 - The reference to the "preparation" of the contract was added in order to cover pre-contractual measures taken at the request of the data subject. However, the Recommendation did not intend to prevent insurance companies from prospecting the market. Insurance companies can, on their own initiative, offer additional insurance cover to existing clients. For instance, an insurer may propose to supplement hospitalisation insurance with a life insurance policy. When an insured person makes travel arrangements, personal insurance may be offered in addition to baggage insurance. In such cases, the provisions of Principle 4.3.*d* may also be applicable.
 - The reference to the "performance" of the contract covers operations carried out by insurers relating to the implementation and the termination of the contract.
 - Finally, the Recommendation is aimed at protecting the rights of persons who are external to but have a link with the contract. It was, therefore, agreed that the processing of data relating to beneficiaries not parties to the contract should be covered on the ground mentioned under Principle 4.3.*d*, or even, where appropriate, 4.3.*c*, the aim being to offer beneficiaries the best possible protection.
 - c.* An alternative condition of lawfulness is the consent of the data subject, his or her legal representative or any authority appointed by law, provided that the collection or processing is not contrary to domestic law. Consent may be given for one or several specified insurance purposes. The controller can lawfully request a single consent for several purposes. The characteristics of consent are dealt with in Chapter 6 of the Recommendation.
 - d.* Lastly, the Recommendation recognises that data collection and processing are lawful when they are in pursuit of a data controller's legitimate interests. For instance, the controller is allowed to collect and to process personal data of the beneficiary of a life insurance policy who is not party to the contract, or even to offer supplementary cover to a client. However, two limits have been imposed on the use of this legal basis. Firstly, the data collected by the data controller must be necessary to these legitimate interests. Secondly, the latter must not be overridden by the data subject's own interests, as full compliance with Chapters 3 and 4 must be guaranteed. In this context, a balance between the interests at stake will have to be struck.

Purpose

46. Principle 4.4 is based on one of the requirements of Article 5 of Convention 108, according to which personal data shall only be processed for specified and legitimate purposes and not be used for incompatible purposes. The first paragraph of Principle 4.4 enumerates the insurance

purposes. The second paragraph of Principle 4.4 recalls the principle of "compatibility". The flexible wording of Principle 4.4 allows for future developments in the insurance sector. Processing may naturally be carried out for a given purpose, even if the latter is incompatible with the original purpose, where, for example, it is provided for by law or if the data subject has nevertheless consented to it, whether or not by contract, and domestic law does not forbid it.

47. The purposes set forth in sub-paragraphs *a* to *k* cover operations carried out by an insurance company, by a financial institution or by an insurance intermediary, in so far as they have an insurance purpose.

a. The purposes set out in sub-paragraphs *a* to *e* concern activities directly linked to insurance benefits. These activities necessitate the collection and processing of personal data for preparing and issuing contracts, paying premiums and other bills, settling claims or paying other benefits, reinsurance or co-insurance.

b. The purposes set out in sub-paragraphs *f* to *k* relate more to data controllers' rights and obligations, particularly:

- preventing, detecting and/or prosecuting fraud (4.4.*f*) in connection with processing carried out by operators in this sector, and in particular insurance companies. When a communication is envisaged, there must be adequate grounds for suspicion before the data controller can specifically process any data, in accordance with Chapter 8;
- establishing, exercising or defending a legal claim (4.4.*g*);
- meeting another specific legal or contractual obligation (4.4.*h*). Legal obligations other than those set out in Principle 4.4.*g* concern, in particular, tax law, social security or the fight against crime. Such obligations can also be contractual. For example, if insurance companies use files other than their client registers for direct marketing purposes, it must be possible to process data to avoid direct marketing aimed at data subjects who do not wish to receive such material;
- the prospecting of new insurance markets (4.4.*i*). This purpose covers cases where global searches are carried out using specific processing methods with a view to identifying new insurance products, in conformity with latent or expressed expectations of the market. In this connection, Recommendation No. R (85) 20 on the protection of personal data used for the purposes of direct marketing stipulates that "*subject to any restrictions laid down by domestic law, any person should be able to collect personal data for direct marketing purposes from files open to the public and other published material*" (see Chapter 2);
- the internal management of an insurance company (4.4.*j*). Examples are: calculating payments to staff and providing information to data subjects to avoid insurance disputes. Another ground stems from the fact that insurance companies need to undertake regular assessments of their insurance portfolios. Such assessments enable them to take management decisions concerning the recruitment of new staff, and staff training. Insurers conclude annual contracts with health-care suppliers. They require certain information for this purpose, for which they first have to analyse personal data collected and processed for insurance purposes;
- actuarial purposes (4.4.*k*). The insurance sector must use actuarial or statistical services, which summarise individual sets of information to highlight the collective features of a given population. They also enable insurers to develop new products. Any processing of personal data conducted in this context is subject to Recommendation No. R (97) 18 concerning the protection of personal data collected and processed for statistical purposes. In particular, the provisions of the Recommendation on statistics require that personal data

collected for statistical purposes should not be communicated to third parties for non-statistical purposes. On the other hand, such data can, under certain conditions, be communicated to third parties with a view to processing for other statistical purposes, because in such cases the purposes are compatible.

In prospecting new insurance markets and for the internal management of an insurance company and actuarial activities, the data must, as far as possible, be used anonymously or at least without means of direct identification, in accordance with the principles in Recommendation No. R (97) 18.

48. The Recommendation refers to the general principle of compatibility of purpose:

- The purpose of the processing must be precisely defined at the time of collection. Defining the purposes of the data reflects three objectives: limiting interference with privacy, ensuring transparency for the data subject and monitoring the purpose of the processing. The purposes listed in Principle 4.4 constitute specific legitimate purposes deriving from the insurance activity, rather than one general purpose.
- One of the purposes could evolve over time. For example, the purposes referred to in Principle 4.1 are the ones listed in Principle 4.4 on "Purpose" but also in Principles 4.8, 8.1 and 13.1 on direct marketing, communication and archiving or conservation. If, at the time of collection, not all the insurance purposes listed in Principle 4.4 have been specified, in accordance with Article 5 of Convention 108, the data thus collected may subsequently be processed for another compatible purpose listed in Principle 4.4, provided it is compatible with the previous purpose(s). For example, data gathered for the purposes of drawing up a motor vehicle insurance policy could be used to prepare a case file in the event of a judicial dispute between the insurer and the data subject bound by the contract. On the other hand, if data are collected for health insurance and medical data are subsequently collected in dealing with claims, a clear picture of somebody's state of health might be the result. Some countries have ruled explicitly that the use of these data for a different type of insurance, such as life insurance, constitutes a form of incompatible use. These data should not be used for the needs of a different insurance branch, such as life insurance.
- In some cases, the question of compatibility arises when data collected for one type of insurance are matched with other data for the purpose of seeking new financial services. In principle, such further use could be regarded as compatible with the original purpose. This further use can also be regarded as compatible when the data are collected by one company of a group (holding or consortium) and used together with the data of another company of the same group, in the exceptional cases where the group itself is the data controller.

Unborn children

49. Principle 4.5, which is based on Recommendation No. R (97) 5 on the protection of medical data, is specifically concerned with the processing of personal data concerning unborn children for insurance purposes. However, it raises ethical issues which go beyond the scope of that Recommendation. The main concern is to protect the privacy of information relating to unborn children after their birth. In most countries, unborn children can be insured. If problems arise and information dating from the pregnancy is collected, the relevant data could be used subsequently. The concern is not to establish parental authority but to ensure that data relating to a child are not already "public" at the time of its birth. The Recommendation advocates the adoption of measures to protect data collected and processed before children are born.

50. Unborn children, therefore, should benefit from similar protection to that afforded to children after their birth. This objective may, for example, be achieved by considering data relating to the

unborn child as personal data of the mother. In accordance with trends in family law in member states, unless otherwise provided by domestic law, those who have parental responsibility for future children should be able to act on those unborn children's behalf as the data subjects. Naturally, when the rights of access and rectification relating to data on the unborn child are exercised, the data subject's interests are duly taken into account.

Sensitive data

51. Principle 4.6 concerns the collection and processing of sensitive data as defined in Chapter 1. It is based on Article 6 of Convention 108, under which such data cannot be processed unless domestic law provides appropriate safeguards. From the standpoint of their purpose, sensitive data are governed by Principles 4.3, 4.4, 4.8, 8.1 and 13.1.
52. Principle 4.6 prohibits the collection and processing of sensitive data. However, exceptions to this principle are allowed for the purposes (and only for the purposes) listed in Principle 4.4. The exceptions are allowed where:
 - a. collection and processing are permitted by law or a supervisory authority - within the meaning of Principle 15.1 - permits it on grounds of an important public interest. In this case, appropriate safeguards must be provided for in domestic law;
 - b. collection and processing are necessary for the purpose of complying with the data controller's specific legal or contractual obligations. In this case again, domestic law must provide appropriate safeguards. However, this exception might not be recognised in certain countries' domestic law, particularly in European Union member states, given that Article 8 of Directive 95/46/EC does not provide for such an exception;
 - c. collection and processing are necessary for establishing, exercising or defending a legal claim;
 - d. collection and processing are necessary for the defence of vital interests of the data subjects themselves or of other persons and insofar as the data subject is not in a position to give his consent;
 - e. it is not contrary to the law and the data subject has explicitly consented to the data processing.
53. In the case of medical data, reference should be made, *inter alia*, to Recommendation No. R (97) 5 on the protection of medical data. A fairly broad definition of medical data was adopted when this Recommendation was drawn up in order to cover all the areas where such data might be used, including that of insurance (see paragraphs 40 and 103 of the explanatory memorandum to Recommendation No. R (97) 5). The authors also bore in mind that data on tobacco use, alcohol abuse and drug taking were also considered to be medical data (paragraph 45 of the explanatory report to Convention 108 and paragraph 38 of the explanatory memorandum to Recommendation No. R (97) 5).
54. With regard to genetic data, reference should also be made to Recommendation No. R (97) 5, which complies with the provisions of the Convention on Human Rights and Biomedicine (ETS No. 164), opened for signature in Oviedo on 4 April 1997. Nevertheless, practice in member states and legal regulations on collection and processing of genetic data for insurance purposes are not uniform everywhere, and so the Recommendation does not prejudge expected developments in this field, particularly in connection with bioethics. For instance:
 - a. Principle 7 of Recommendation No. R (92) 3 on genetic testing and screening for health care purposes states that "Insurers should not have the right to require genetic testing or to

enquire about results of previously performed tests, as a pre-condition for the conclusion or modification of an insurance contract".

- b.* To date, however, the various European countries have adopted different positions on the collection and processing of genetic data for insurance purposes. In some countries, for instance, where an insurance contract involves large sums, it is deemed permissible for the insurer to request communication of the results of predictive genetic tests. In other countries, the use of genetic data for insurance purposes is purely and simply prohibited by law. Lastly, yet other countries have proclaimed a moratorium on the subject.
- c.* Principle 4.9 of Recommendation No. R (97) 5 provides that "For purposes other than those provided for in Principles 4.7 (for preventive treatment, diagnosis or treatment) and 4.8 (for the purpose of a judicial procedure or a criminal investigation), the collection and processing of genetic data should, in principle, only be permitted for health reasons and in particular to avoid any serious prejudice to the health of the data subject or third parties (...)".
- d.* Article 12 of Convention No. 164 states that predictive genetic tests may only be performed for health or medical research purposes, but does not specify whether the use of such tests is authorised for other purposes, including those relating to insurance. Would such a use entail discrimination against individuals on grounds of their genetic heritage (Article 11) or stand in the way of equitable access to health care (Article 3), thus infringing the principle of human dignity? Such a use of genetic data might possibly be subject to the restrictions set out in Article 26 of the same Convention for reasons, for instance, of protection of other persons' rights and freedoms. However, Article 5 of Convention 108 does not exclude the possibility of genetic data collected for health or medical research purposes being used for other, compatible, purposes. These issues lie halfway between "bioethics" and "infoethics", and are being examined specifically by the Council of Europe committees responsible for drawing up an additional protocol on genetics to Convention No. 164. Restrictions on the collection and processing of genetic data imposed by this additional protocol will apply equally to personal data collected and processed for insurance purposes. It is for that reason, in particular, that no provision on genetic data was included in this Recommendation.

Criminal data

- 55. Principle 4.7 is aimed at reinforcing the protection of one particular category of personal data, namely data relating to criminal proceedings and convictions. These categories of data are also collected and processed in the insurance field. However, they can only be processed if they are needed for the actual existence and operation of insurance. For example, for some forms of insurance, the insurer may need to ascertain whether the insured person has been convicted of criminal offences.
- 56. The Recommendation authorises the collection and processing of such data for insurance purposes, if:
 - a.* the processing is in accordance with appropriate safeguards provided for in domestic law;
 - b.* it is necessary for achieving the legitimate purpose of data collection. This is a particular application of the proportionality principle set out in 4.1. However, this application requires the precise reason for collecting the data to be specified with the greatest clarity;
 - c.* the purpose of collecting and processing such data is concerned with one of a limited number of purposes, namely:
 - preparing and issuing insurance contracts (4.4.a);

- settling claims or paying other benefits (4.4.c);- combating insurance fraud (Principle 4.4.f).

Direct marketing

57. Principle 4.8 lays down special rules governing the collection and processing of personal data in the insurance field for direct marketing purposes. It is intended to permit a certain amount of prospecting among persons on whom data have already been collected or processed by the data controller for the purposes of insurance.
- According to the Recommendation, personal data should be collected and processed for direct marketing purposes only if the data subject has not objected and only after he/she has been fully informed of this action in accordance with Chapter 5:
 - Data collection and processing for direct marketing purposes for the range of services at the data controller's disposal are subject to the opting-out system. In this system, the data controller can collect and process data for direct marketing purposes without any obligation to ask for the data subject's consent, provided that the data subject has the opportunity to object.
 - Increasing numbers of groups and companies are providing insurance services as well as other services. It is, therefore, not always easy to define the precise boundaries of such a group or company beyond which any information passed on constitutes communication to a third party. This is why communication of such data is specifically governed by Principle 8.1.c of the Recommendation, which also provides for the opting-out system. This solution is based on Recommendation No. R (85) 20 on the protection of personal data used for the purposes of direct marketing, which draws a distinction between data collection for direct marketing purposes and the making available of lists to third parties.
 - In accordance with Chapter 5, data controllers do not themselves have to inform data subjects of their right to object to the processing of their data for direct marketing purposes, but can inform them of this right via general information to the public.
 - The recommendation does not aim to exclude the use of sensitive data for direct marketing purposes, nor to prohibit insurance companies from drawing up profiles. Nevertheless, the use of sensitive data requires data subjects' explicit consent (in accordance with Article 8.2.a of the Directive), provided that domestic law does not prohibit the processing even where the data subjects have consented, in accordance with Chapter 6 on consent. This extends also to providing such consent over the telephone, in the case of telephone surveys.

5. Information for the data subject

58. Chapter 5 is concerned with the information that data controllers must supply to data subjects in order to comply with the fairness requirements in Article 5 of Convention 108. The Recommendation draws a distinction between this type of information and other categories of information considered in Convention 108:
- Article 8 of Convention 108 entitles individuals to obtain information on any personal data concerning them that have been recorded or communicated, and if appropriate to ask for these data to be amended, with a right of appeal. These are additional safeguards designed to enable everyone to defend their rights in response to computerised files, given the danger that individual decisions concerning them could be taken on the basis of data either contained in these files or communicated to third parties by a data controller.
 - Pursuant to Article 5 of Convention 108, persons about whom data are collected must, as a matter of principle, receive immediate relevant information concerning the nature,

characteristics, circumstances and purposes of the data collection and processing. Such information is not only critical for the fairness of the data collection and processing but also a way of obtaining honest, and therefore reliable, data. The fairness of the collection process and the quality of the data gathered for insurance purposes are, therefore, linked.

59. Sub-paragraphs *a* and *b* of Principle 5.1 detail the information that must always be supplied to data subjects. In every case, the data subjects must be told the purpose or purposes for which the data were being or would be processed and the identity of the data controller. However, the obligation to provide information should not place a disproportionate burden on data controllers as compared with the purposes of the data. This is why the Recommendation therefore presents a minimum list under sub-paragraph *c* of other information that must, if appropriate, be supplied to data subjects to ensure the fairness of collection, within the meaning of Principle 5.4. In particular, data subjects should, where necessary, be informed of the categories of data collected or to be collected; the categories of external persons or bodies to whom, and the purposes for which, they may be communicated; the possibility, if any, for data subjects to object, for example to the processing of their data for direct marketing purposes and to refuse their consent or withdraw it and the consequences of such withdrawal; the conditions under which the rights of access and of rectification may be exercised; and the categories of any other sources which may be consulted.
60. Principle 5.2 concerns information for data subjects where the data are collected from the subjects themselves. It states that information must be communicated at the latest at the time of collection, unless the data subjects have already received the information by other means. This exception to the duty to provide information, because the data subject has already been informed, should be interpreted strictly. In the case of telephone selling, for example, informing persons at the start of conversations of the possibility that data will be collected and processed is not sufficient in order to be applicable to all possible future contractual relationships. However, it might be acceptable not to supply such information if this has already been done in writing shortly before, in the course of negotiations concerning the same contract.
61. Principle 5.3 is concerned with cases where data are collected from third parties. It stipulates that data subjects must be informed of this by one means or another, either as soon as the data are recorded, or, if it is intended to communicate data to a third party, at the latest when the data are first communicated.
62. The provision of information on this form of data collection clearly cannot take place under the same conditions as those pertaining to collection from the data subjects. The obligation to inform data subjects has to be adapted to the particular circumstance of data collection for insurance purposes from third persons. In particular, besides the fact that there is no point, as in the case of collection from data subjects, in informing them again when it is clear that they have already received the information set out in Principle 5.1, derogations to information provision are provided for when in practice such provision is manifestly unreasonable or impracticable, or when the collection or processing of data for insurance purposes is expressly provided for in domestic law. In the last two cases, domestic law must specify appropriate safeguards, which must be applied by data controllers. These could, for example, take the form of general types of publicity.
63. In Principle 5.4, excessively detailed information may place a disproportionate and unnecessary burden on both the insurance industry and data subjects. The information supplied by data controllers should, therefore, be commensurate with the data subjects' interests, the circumstances, the implications and the scope of the data collected. In particular, the terminology used and the level of detail or generality of the information should be such as to offer the person questioned an overall grasp of the purpose and significance of the data collected. The information supplied by the data controller is particularly relevant to any

assessment of the fairness of the collection process. Lastly, there should be sufficient information to enable data subjects to give their informed consent, where consent is the basis for lawfulness of processing.

64. Principle 5.5 is concerned with information collected for insurance purposes in the case of data subjects with no legal capacity. These are persons who under domestic law are unable to act in their own name. They include both minors and persons unable to exercise judgement, who are therefore unable to give their free and informed refusal or consent.
- a. When personal data are collected about persons who have no legal capacity, the relevant information clearly has to be supplied to their legal representatives. However, some member states' domestic law authorises certain categories of persons lacking legal capacity to act in their own names and, in these particular cases, the information can be supplied directly to the data subjects themselves.
 - b. Principle 5.5 also stipulates that persons who lack legal capacity but are nevertheless able to understand what is involved must be informed directly. In certain particularly sensitive areas, such as life assurance, this information is important for ensuring that consent is genuinely freely given.
65. Principle 5.6 is based directly on Article 9 of Convention 108, which sets out the authorised limits to any interference in the rights enshrined in Convention 108. Convention 108 allows derogations from information provision when such derogations are provided for by law and are necessary measures in a democratic society in the interests of certain legitimate aims, which are listed. This wording derives directly from the second paragraph of Article 8 of the European Convention on Human Rights, but the aims set out in the Recommendation do not include national safety, public security or the country's monetary interests. Thus, the provision of information could be restricted if this is necessary for a data subject's protection or to protect the rights and freedoms of others. Restricting the information supplied to beneficiaries of, for instance, a life insurance contract may be based on the right of insured persons to respect for their privacy.

6. Consent

66. Chapter 6 concerns consent by data subjects where they have the option of granting or refusing permission for data concerning them to be collected or processed for insurance purposes. This chapter is based on Article 5 of Convention 108 and Principle 4.3 of the Recommendation, whereby consent is one of the essential conditions for data collection to qualify as fair and lawful. It should be remembered here that the type of consent peculiar to data protection must be distinguished from the conditions for validity of consent in the context of a contract. Furthermore, Principle 4.3 of the Recommendation clearly considers the contract and consent as separate bases for lawfulness.
67. Principle 6.1 defines the characteristics and general rules of consent. A data subject's consent must be "given freely, unambiguous, specific and informed." It must also be given in a manner that precludes any doubt.
- a. Consent must, therefore, concurrently satisfy four criteria:
 - since it is free, it must not have been obtained under coercion or excessive influence or pressure;
 - since it is "specific", such consent must relate to one or more given data-processing operations and must not be construed as blanket permission granted by the data subject to the data controller, unless the data subject has unambiguously intended to give such a blanket permission for one or more operations;

- since it is "informed", such consent means that the data subject has been informed in advance of the purposes and procedures of the data collection and processing to which he or she is consenting, in accordance with Chapter 5 of the Recommendation;
- since it precludes any doubt, it is not sufficient to consider that the data subject is presumed to have given his/her consent.

b. The consent must be given in an even stricter form in cases of collecting and processing "sensitive data", as defined in Chapter 1; in such cases, the consent must be given by the data subject not merely in a manner that precludes any doubt as described in the previous sub-paragraph but explicitly, which involves securing an express manifestation of the data subject's will. There may be cases where domestic law provides that the prohibition of collection or processing of sensitive data may only be raised with the consent of the data subject. This is the case in some countries with regard, for instance, to processing of medical or genetic data.

68. Principle 6.2 relates to consent in cases where data collected or processed for insurance purposes concern persons without legal capacity. In principle, consent, as defined in Principle 6.1, must be given by the person legally responsible for the data subject (parents, a guardian or any other person, authority or body assuming legal responsibility for the data subject under the law). However, where domestic law provides that certain categories of persons without legal capacity may act on their own behalf, such persons may themselves give or refuse consent. In accordance with Principle 5.5, which recommends informing persons who lack legal capacity but are capable of understanding, the authors took the view that, except where prohibited under domestic law, such persons should be given an opportunity to state their wishes on the subject of taking out or not insurance. This is not a matter of consent in the strict sense of the word (since the final decision lies with the person legally responsible), but of a measure aimed at involving these data subjects in the discussion and the decision-making process *vis-à-vis* consent.
69. Principle 6.3 specifies that, where possible, consideration should be given to the wishes of persons legally considered as lacking capacity when, for instance, they have been informed of the collection and processing of data concerning them and have been able to understand, unless otherwise stipulated by domestic law.

7. Collection and processing by processors

70. Chapter 7 lays down specific rules on the conditions under which data controllers can contract out the collection or processing of personal data for insurance purposes. Obviously, contracting out is possible only if it does not breach legal or contractual obligations in matters of security or confidentiality.
71. Principle 7.1 refers to the possibility for data controllers as defined in Chapter 1 to delegate collection and processing of personal data for specific insurance purposes to a processor, who may generally be any natural or legal person, public authority, agency or organisation, provided that such processor undertakes to act solely under the instructions of the data controller and to abide by the principles set forth in Chapter 11 on security.
72. Principle 7.2 lays down the obligations incumbent on controllers where the choice of processor is concerned. For instance, they must choose processors who offer adequate safeguards concerning the technical and organisational aspects of processing. The relevant measures are specified in Chapter 11 of the Recommendation, on data security. Lastly, it is mandatory for controllers to ensure that collection and processing are performed in accordance with their instructions.

73. One logical consequence of the above is the requirement, set forth in Principle 7.3 of the Recommendation, that processing should be governed by contract or by any other legal instrument needed to give substance to the above-mentioned obligations. It is also clear that data controllers are still required to fulfil all the obligations set out in the Recommendation in respect of any processing contracted out to a processor.

8. Communication for other purposes

74. This chapter lays down the conditions whereby personal data collected and processed for the purposes provided for in the Recommendation may be communicated to third parties for further processing for other than insurance purposes.

- a.* Firstly, according to the definition in Chapter 1, communication is a form of processing. Consequently, any communication of personal data must be carried out in accordance with all the principles enshrined in the Recommendation.
- b.* In addition to the purposes specified in Principle 4.4, communication is permissible:
 - where provided for by law, on important public interest grounds, such as the suppression of crime. Under Article 9 of Convention 108, since it amounts to an interference with privacy, such communication is allowable only where provided for by law and where it constitutes a measure necessary in a democratic society for one of the purposes set forth therein;
 - where the data subjects have given their consent, under the conditions set out in Chapter 6, and communication is not prohibited by domestic law;
 - for prospecting purposes under the conditions set out in Principle 8.c; nevertheless, Recommendation No. R (85) 20 on the Protection of Personal Data used for the Purposes of Direct Marketing provides that where lists are made available to third parties, "Unless the data subject has given his consent, the lists should not provide any information liable to infringe his privacy". This might apply, for instance, to profiles revealing certain characteristics of the data subject;
 - in the legitimate interests of the controller, in accordance with and under the conditions set out in Principle 4.3.d.

9. Individual automated decisions

75. Individual automated decisions are decisions taken solely on the basis of automated data processing, enabling data subjects to be categorised according to pre-established criteria or statistical results. Individual automated decisions are commonplace in the insurance industry, and are sometimes necessary for the good of data subjects and of customers.

76. Principle 9.1 institutes a ban on certain individual automated decisions which have legal effects on data subjects or affect them significantly. Examples are decisions on granting or extending insurance or the payment of other benefits. However, the mere fact of sending advertising leaflets to a list of specified persons by computer would not constitute a decision liable to be prohibited pursuant to Principle 9. Such a decision must also have been taken on the sole basis of automated processing: what is prohibited is the strict application by the user of the results obtained by the software or expert system without any room for human appraisal. Computers can obviously be used to help the decision-making process, for example in evaluating the risk for which the person in question is requesting insurance cover.

77. The Recommendation provides therefore that such decisions shall be permissible where they are taken in response to a request made by the data subject with a view to the conclusion or execution of an insurance contract or where data subjects are permitted to express their point of view in order to guarantee protection of their legitimate interests. Such decisions may also

intervene if they are provided for by the legislation stipulating measures to protect data subjects' legitimate interests.

10. Rights of access and rectification

78. Chapter 10 deals with the rights conferred under Article 8 of Convention 108: all data subjects must know if data concerning them have been obtained and are held by the data controller. They must have right of access to personal data concerning them and must be able also to require the controller to rectify data which prove to be inaccurate or outdated. The aim of this chapter is to permit data subjects to protect themselves against the risk that individual decisions or measures concerning them may be based on inaccurate or outdated data contained in any files which have been or could be communicated to third parties by the controller. The data subject must be able to exercise freely his/her right of access; for example, no third party must require the data subject to exercise his/her right of access in order to communicate the data to this party or to another person. Moreover, the authors of the Recommendation stressed that the data subject must be able to exercise the right of access without infringing business secrecy or intellectual property, for example copyright *vis-à-vis* the software, particularly in cases of information on the reasoning behind the automated processing. It goes without saying that data subjects should exercise their right of access reasonably and avoid making over-frequent or otherwise vexatious requests.
79. Principle 10.1 lists the information which data subjects must be able to access on request. It includes:
- a. confirmation that the relevant data are, or are not, being collected or processed;
 - b. in an intelligible form, relevant data and information concerning at least:
 - the purposes of the processing operation;
 - the categories of data concerned by the processing;
 - the recipients or categories of recipients to whom the data are communicated;
 - the source of the data. Information on the source of the data must only be provided if it is available.
 - c. knowledge of the reasoning behind the automated processing of his/her data, at least in the case of an automated individual decision.
80. Principle 10.2 reiterates a derogation provided for in Article 9 of Convention 108, which stipulates that access to personal data may be restricted for the purpose of suppressing crime, or to avoid jeopardising the outcome of an inquiry in progress. Chapter 4 provides for collection of data for the purpose of detecting and/or prosecuting fraud. On completion of an inquiry, the controller must inform data subjects that their data are now accessible. The authors nevertheless considered cases where restriction of access must continue without it being able to be said if and when the restriction will be lifted.
81. Principle 10.3 relates to the right of data subjects to have their insurance data erased, blocked or rectified where they prove to be inaccurate or irrelevant. In some cases, rectification alone does not suffice, and to repair the damage done to the data subject, or to restore conditions of fair processing, it may be necessary to delete or even destroy or block data. Principle 10.5 states that where controllers have communicated such data, they must also notify the recipients of any rectification, deletion, destruction or blocking which they carry out, except where this requirement is manifestly unreasonable or impracticable.
82. Principle 10.4 provides that data subjects must be notified in writing of any limitation or refusal of the right of access, rectification, deletion or destruction of data, along with the grounds for the decision, unless explaining the grounds would prejudice the reason for refusing access. This

applies, in particular, to cases where access is refused or deferred pursuant to Principle 10.2. In such cases, data subjects should be informed of their right to submit the case to the relevant supervisory authority. Furthermore, under Article 5.d of Convention 108, controllers are required to update data, where necessary.

- 83. Principle 10.5 provides that controllers must inform any third parties to whom they have communicated data of an individual that these data have been rectified, erased or blocked, unless this is manifestly unreasonable or impracticable.
- 84. According to Principle 10.6, the data controller must allow data subjects to exercise their right of access "without excessive delay or expense". The controller may also exempt the exercise of this right from any charge. The person who exercises the right of access may be the data subject or his/her legal representative. This person is entitled to request any necessary information on the processing and on the data subject's data.

11. Security of data

- 85. Principle 11.1 relates to the technical and organisational measures that must be taken to guarantee data security. Data security encompasses the confidentiality, integrity and availability of data. In order to guarantee full protection of personal data, material precautions must be taken by controllers to prevent unlawful access to or use of data, whether accidental or ill-intentioned. The technical and organisational measures must also be periodically reviewed. Having regard to the state of the art and the cost of implementing such measures, they must guarantee a level of security suited to the risks arising out of the processing and the nature of the data to be protected.
- 86. The security measures required under Principle 11.2 cover the powers and authorisations of departments and individuals responsible for security. They also include measures concerning access to installations and documents (*a, b, c* and *e*), transport and transfer of data media (*d, f* and *h*) and, lastly, procedures, logical keys, processing programmes, and data encryption and scrambling (*g* and *i*). The Recommendation presents an explicit list of security measures needed to guarantee the confidentiality, integrity and accuracy of data. This constitutes a minimum list of measures in conformity with national and international data protection standards.
- 87. Principle 11.3 follows logically from the preceding principle. It requires controllers to draw up internal regulations setting forth the technical and organisational measures to be implemented in order to meet the data protection requirements of this Recommendation. In this connection, it should be said that security measures are incumbent on recipients of personal data communicated for insurance purposes as much as on controllers and their processors. It is mandatory for a controller to inform all persons involved in data collection and processing of their duties in this respect. Such persons must formally undertake to comply with security measures.
- 88. Principle 11.4 relates to the option open to firms to appoint a person responsible for supervising their in-house application of data protection principles. That person, who should not discharge any duties incompatible with this supervisory function, would advise the firm on all data protection matters, in particular the technical and organisational measures to be taken, and will represent it in dealings with the national data protection authorities.

12. Transborder data flows

- 89. Principle 12.1 relates to international flows of personal data being used for insurance purposes. The need to strike a balance between free movement of information and respect for privacy also applies to transborder communication of personal data. Indeed the growth of individual mobility and the globalisation of economic activity are generating an increased need for information.

Developments in information and telecommunications technology have a decisive impact on the insurance industry. Insurers must, therefore, be careful to ensure that data are protected, whatever the medium used for data transfer, including the information highways.

90. Principle 12.2 shows how Article 12 of Convention 108 applies to transborder flows of insurance data. It deals with countries that are parties to Convention 108 and which have equivalent data protection legislation. There is no reason to restrict transborder flows of insurance data between persons, firms or public or private institutions located in the territory of those parties. Transfers of insurance data to a third state via the territory of a party to Convention 108 must not be used as a means of circumventing the data protection legislation in force.
91. Principle 12.3 also allows transborder flows of insurance data from states implementing this Recommendation to persons, firms or institutions located in states parties to Convention 108 and persons, firms or institutions located in the territory of states which ensure an adequate level of protection.
92. Principle 12.4 deals with transborder flows of personal data for insurance purposes to states which do not guarantee adequate protection. Except where the domestic law of the sending state provides otherwise, such data flows should not as a rule occur unless one of the following two conditions is met:
 - a. either data subjects have been informed that data concerning them may be transferred to a state which does not offer guarantees of protection equivalent to those in force in their own country and the data subjects have unambiguously given their consent to such a data flow;
 - b. or specific measures have been taken, in particular by contractual agreement, to ensure that the protection and security measures implemented are in keeping with the principles of Convention 108 and the Recommendation.

13. Conservation of data

93. Principle 13.1 concerns the storage and destruction of personal data collected for insurance purposes.
 - a. In accordance with Article 5.e of Convention 108, this principle requires that data be destroyed or deleted as soon as they are no longer needed for the purpose for which they were collected and processed. Firms storing data must not delete them with a view to destroying evidence likely to prove their liability, while claiming that they are merely complying with this principle. This refers to certain special cases, such as the despoilment of Jewish assets during the Second World War and the use of firms' private archives in order to compensate the victims.
 - b. The principle also allows the conservation of data for statistical or scientific research purposes, or for other purposes provided for by law. Research by historians comes naturally within the ambit of scientific research. In this respect, it is true that a growing number of firms are setting up their own archives, which are used extensively by historians. In this case, insurance data being kept for the above purposes must be covered by sufficient guarantees, for example by storing them separately and making certain data accessible only for those purposes.
94. Principle 13.2 points out that it may be in the insurers' interest to keep data on persons to whom they have refused cover, in particular as a means of preventing fraud. Furthermore, although time-limits on storage are not easy to establish, they are, nonetheless, necessary to prevent abuse and the creation of long-lasting "blacklists".

14. Remedies

95. This principle reiterates the provisions of Article 10 of Convention 108. Although special rules adopted by the industry itself are useful as a means of guaranteeing effective protection, appropriate sanctions and remedies must be provided under domestic law. Whether such sanctions and remedies are civil, administrative or criminal in nature will depend on each state's own legal system. However, an appropriate remedy also entails the possibility of appealing to a national authority, as provided for in Principle 15.1.

15. Ensuring respect for the principles

96. Principle 15.1 requires each state to establish an independent supervisory authority, except where such an authority already exists and has jurisdiction to deal with breaches of the domestic law implementing the principles laid down in the Recommendation. Most countries will have established such supervisory authorities on passing a data protection law.
97. Principle 15.2 enshrines an additional guarantee of compliance with data protection principles. It requires controllers to make public by appropriate means - for instance in the press - the processing operations carried out and, in particular, the nature of the principal data being processed.

Note 1. There are currently forty-four member states: Albania, Andorra, Armenia, Austria, Azerbaijan, Belgium, Bosnia and Herzegovina, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Georgia, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Liechtenstein, Lithuania, Luxembourg, Malta, Moldova, Netherlands, Norway, Poland, Portugal, Romania, Russian Federation, San Marino, Slovakia, Slovenia, Spain, Sweden, Switzerland, "the Former Yugoslav Republic of Macedonia", Turkey, Ukraine, United Kingdom.

Note 2. *Z. v. Finland*, judgment of 25 February 1997. This case law was confirmed in the judgments *M. S. v. Sweden* of 27 August 1997, Rec. 1997, *Amann v. Switzerland* of 16 February 2000, Rec. 2000, *Rotaru v. Romania* of 4 May 2000, Rec. 2000.

Note 3. Hereafter referred to as "Convention 108".

Note 4. Austria, Belgium, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Netherlands, Norway, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden, Switzerland and the United Kingdom.

Note 5. Bulgaria, Georgia, Moldova, Russian Federation and Turkey.

Note 6. Since 1989, the Council of Europe has elected its own Data Protection Commissioner, who supervises the protection of personal data within the Secretariat General.

Note 7. 1. Recommendation No. R (99) 5 for the protection of privacy on the Internet (23 February 1999)

2. Recommendation No. R (97) 18 concerning the protection of personal data collected and processed for statistical purposes (30 September 1997)

3. Recommendation No. R (97) 5 on the protection of medical data 13 February 1997)

4. Recommendation No. R (95) 4 on the protection of personal data in the area of telecommunication services, with particular reference to telephone service (7 February 1995)

5. Recommendation No. R (91) 10 on the communication to third parties of personal data held by public bodies (9 September 1991)
6. Recommendation No. R (90) 19 on the protection of personal data used for payment and other related operations (13 September 1990)
7. Recommendation No. R (89) 2 on the protection of personal data used for employment purposes (18 January 1989)
8. Recommendation No. R (87) 15 regulating the use of personal data in the police sector (17 September 1987)
9. Recommendation No. R (86) 1 on the protection of personal data used for social security purposes (23 January 1986)
10. Recommendation No. R (85) 20 on the protection of personal data used for the purposes of direct marketing (25 October 1985)
11. Recommendation No. R (83) 10 on the protection of personal data used for scientific research and statistics (23 September 1983) replaced by the aforementioned Recommendation No. R (97) 18 on data used for statistical purposes.
12. Recommendation No. R (81) 1 on regulations for automated medical data banks (23 January 1981), replaced by the aforementioned Recommendation No. R (97) 5.

Note 8. New technologies: a challenge for privacy? (1989)

Data protection and the media (1990)

Personal identification numbers: their implementation, use and data protection (1991)