Explanatory Memorandum
Recommendation No.R (90) 19 of the Committee of Ministers to Member States concerning the protection of personal data used for payment and other related operations

(Adopted by the Committee of Ministers on 13 September 1990 at the 443rd meeting of the Ministers' Deputies)

INTRODUCTION

1. The impact of data processing technology on various public and private sector activities has long engaged the attention of the Council of Europe's Committee of experts on data protection (CJ-PD), the intergovernmental body which was responsible for the elaboration of what is still the world's only binding legal instrument in the field of data protection - the Convention for the protection of individuals with regard to automatic processing of personal data of 28 January 1981 ([1]). Focussing on particular data processing contexts has enabled the Committee of experts to provide detailed principles and guidelines for the protection of individual privacy based on the provisions of the Convention but adapted so as to have concrete meaning in those contexts.

2. The guidelines and principles have taken the form of recommendations adopted by the Committee of Ministers on the basis of the drafts prepared by the Committee of experts and its Working Parties. These recommendations are addressed by the Committee of Ministers to the governments of the member States, inviting them to take account of the solutions offered in the recommendations when they are dealing with the particular data protection issues discussed in the recommendations.

3. Six such initiatives have so far been taken in the framework of what is now commonly referred to as the "sectoral approach" to data protection.

- Recommendation No. R (81) 1 on regulations for automated medical data banks (23 January 1981);
- Recommendation No. R (83) 10 on the protection of personal data used for scientific research and statistics (23 September 1983);
- Recommendation No. R (85) 20 on the protection of personal data used for purposes of direct marketing (25 October 1985);
- Recommendation No. R (86) 1 on the protection of personal data used for social security purposes (23 January 1986);
- Recommendation No. R (87) 15 regulating the use of personal data in the police sector (17 September 1987);
- Recommendation No. R (89) 2 on the protection of personal data used for employment purposes (18 January 1989).

4. The Committee of experts has now turned its attention to various data protection issues raised by the impact of data processing technology on personal information generated by the supply and use of payment media. The cashless society has been promoted by the widespread use of cheques for settling transactions. It is now being furthered by the proliferation of plastic cards. Technology has now made it possible to speak in terms of electronic money by

providing electronic funds transfer at point of sale through use of terminals installed either on retailers' premises or in the home. Payment cards are themselves becoming "intelligent" now that it is possible to integrate microprocessors into them.

5. It fell to a specially constituted Working Party of the Committee of experts on data protection to examine the consequences of these developments on payment media on the collection, storage and processing of personal data. Under the Chairmanship of Mr. J.-P. WALTER (Switzerland), this Working Party met on five occasions between June 1987 and January 1989 "to examine the data protection problems posed by certain aspects of the banking sector, in particular the use of smart cards, point of sale transfers, etc.".

6. With the support of the plenary Committee, the Working Party focussed its attention on the automatic processing of personal data which are collected and stored pursuant to the provision or use of means of payment. This broad approach allowed it to examine not simply the issues raised by smart cards and electronic funds transfer (as specifically identified in the mandate) but also other types of technology which are used for settlement operations (for example, home banking terminals, automatic cash dispensers). Indeed, since the point of departure was constituted by the automatic processing of personal data in the area of means of payment or other related operations, the Working Party could not avoid devoting attention to non-technology based payment media (for example cheques and traditional payment cards) since their use may give rise to automatic processing of personal data at a later stage. Nor could the Working Party overlook the whole range of bodies now offering means of payment to clients and which are not banking institutions in the strict sense of the term. In addition, given that the new electronic payment media no longer give rise to a discrete relationship between the body providing them and the user, it was felt necessary to include within the framework of the inquiry the complete range of actors who may intervene in the course of payment or related operations and who may be obliged to collect and store personal data: beneficiaries of transactions, network operators and all types of bodies providing means of payment.

7. It was against this background that the Working Party noted the increase in circulation of personal data within this sector given the diminishing importance of cash transactions. This was borne out by the increase in bodies, other than banks stricto sensu, which were making payment media available to a public increasingly willing to acknowledge their advantages over cash. The Working Party noted inter alia that these developments increased the potential for the profiling of consumer habits since payment media tended to leave behind traces of spending behaviour each time they were used. Data processing made it possible to build a cumulative picture of isolated consumer transactions.

8. The multiplicity of actors involved, coupled with the fact that a large number of bodies providing means of payment were not subject to principles of banking supervision, added further difficulties. The transnational character of settlement operations via payment media could not be overlooked either.

9. While noting that the Convention applied to personal data processing in this whole area, the Working Party nevertheless felt the need to elaborate a set of fair information practices designed to minimise the possible privacy risks for the individual through the provision and use of payment media. Using the approach followed for previous sectors, the Working Party, in close consultation with the plenary Committee of experts, adapted the principles contained

in the Convention so as to regulate the various stages where data protection is seen as crucial: collection, storage, use, communication and conservation of personal data. The Working Party also sought to provide for the rights of the data subject in this sector and offered a solution to minimise the privacy risk caused by personal data being transferred between countries.

10. The draft principles emerging from the Working Party's discussions were examined at length at the 17th meeting of the Committee of experts on data protection (7-10 March 1989). The Committee eventually gave provisional approval to them, while allowing its members to propose further amendments in advance of the 18th meeting. The Secretariat was instructed to draw up a draft explanatory memorandum for examination and approval at the 18th meeting.

11. On the basis of a series of written comments and observations submitted by several delegations on both the draft recommendation and the draft explanatory memorandum, the Committee once again examined both these texts at its 18th meeting (3-6 October 1989). It was felt that the amendments made to these texts in the course of that meeting should be carefully thought over by the experts before final approval could be given to them. For this reason, the experts were invited to reflect once more on the drafts in advance of the 19th meeting of the plenary Committee, and to submit observations in writing in regard to the new amendments.

12. At its 19th meeting (20-23 March 1990), the Committee approved both texts and subsequently forwarded them to the European Committee on Legal Co-operation for examination and adoption. The draft recommendation and draft explanatory memorandum were approved by the CDCJ on 11 May at its 53rd meeting from 8-11 May 1990. Recommendation no. R (90) 19 on the protection of personal data used for payment or other related operations was adopted by the Committee of Ministers of the Council of Europe on 13 September 1990.

Detailed comments

Preamble

13. As with other organisations in the public and private sectors, bodies providing means of payment have benefited greatly from the technological revolution, in particular from data processing techniques. Referring to "bodies providing means of payment", for example banks, but not necessarily so, data processing allows for more effective and speedier account management. It allows a better service to be given to the client. It allows for settlement operations to be processed more rapidly.

14. At the same time, telematics, which has brought together the benefits of the computer and the benefits of telecommunications, has allowed the individual to profit from a whole new range of financial operations. With the necessary hardware, as well as a data transmission link, the individual can interrogate from his domicile the state of his account. He can order chequebooks, or give instructions to his bank to make a standing order in favour of a beneficiary. Automatic cash dispensers or tellers allow him similar facilities, including the withdrawal of cash. Point of sale terminals located in the premises of retailers, traders and service providers allow the individual to debit electronically his account and instruct the bank to credit the account of the beneficiary of the transaction.

15. In addition to the hardware, a whole range of electronic payment cards are now in circulation, some of which are necessary to allow the transactions referred to in the previous paragraph to be carried out. Some of these cards are more sophisticated than others. The smart card, or microchip card, may integrate the qualities of the credit card, the debit card and cheque guarantee card, and at the same time provide an entry into the automatic teller machine or point of sale terminal.

16. The Preamble recognises all the advantages which automated data processing has brought to the area of means of payment and other related operations. The benefits do not accrue exclusively to banks and other bodies which provide means of payment. From the point of view of the retailer operating a point of sale terminal, he is paid more quickly. The amount of cash which he is obliged to keep on his premises is reduced. His book keeping problems are eased. From the point of view of the individual, electronic payment cards provide him with 24-hour access to banking facilities. He is not obliged to carry large sums of money.

17. At the dawn of the cashless society, it is felt appropriate to reflect on the consequences which data processing within the means of payment sector may have on the individual's private life. Private life is not to be seen exclusively in terms of intrusive conduct. Rather, for the purposes of this Recommendation, it is to be understood in terms of his ability to control and monitor third party collection, storage and use of the personal data which he releases in the course of a transaction. It is the case that cashless and paperless transactions give rise to records where none existed previously.

Payment by cash, and therefore the absence of documentation, has the advantage that the individual can maintain his anonymity. To all intents and purposes, the informational value of a cash transaction is zero, since the individual leaves few traces behind either in regard to the nature of the transaction or his identity. However, the new payment media are characterised by data storage and by the intervention of various different parties. Electronic payment media have the potential to reveal a considerable quantity of personal data by the fact of their use. Once that data are collected and stored by third parties, data processing techniques can be brought to bear on them so as to enable isolated, fragmented uses of the means of payment to be brought together in the form of a profile which can allow the individual's economic and consumer behaviour, and even his movements, to be monitored. It is these sort of risks which are the subject of the guidelines contained in the Recommendation.

18. Banks in the strict sense of the term no longer enjoy a monopoly over the provision of payment media. Bodies such as department stores and petrol companies also provide their own company-specific cards, some of which may be used in a point of sale terminal located in their subsidiary's premises. The Preamble notes that the latter bodies are not bound by principles of banking secrecy which do serve as a useful complement to data protection principles in so far as the communication of data is in issue. However, it is to be recalled that data protection is a broader concept than banking secrecy, referring as it does to all the various data processing stages and not simply the communication stage.

19. The Data Protection Convention, as well as national data protection legislation, applies to data processing accompanying the provision or use of a means of payment and to all the actors involved in this sector. However, as the Preamble states, it has been felt appropriate to define more precisely the general Convention norms so as to make them more meaningful to the way

in which personal information circulates in the means of payment sector and to the way in which data processing may affect it both qualitatively and quantitatively. It is for this reason that the Recommendation puts forward principles on how personal data should be collected and stored, how they should be used, the circumstances which should govern their communication, their security, their conservation, as well as on the rights of the individual data subject in regard to his data. It is felt that these principles are an informed and studied response to the problems which may arise out of automatic processing of personal data as a result of the provision of a means of payment and of its use.

20. The text is not confined to "electronic money". It will be seen from the scope and definitions section that cheque and plastic card transactions are covered by the principles. It is after all the case that the provision and use of such means of payment will give rise to data collection and storage. They have an informational value when used. What is important is not the medium used for payment, rather the fact that its use involves automated processing of personal data at the time of use or at a later date.

21. Although the Preamble makes a plea in favour of preserving the anonymity of the parties to the operation despite the increasing recourse to electronic payment media, the text is not advocating the right of the individual to settle his transactions in cash. The authors of the Recommendation are simply suggesting that the individual should always be able to choose between settling his transactions in cash (and he may have good reason to maintain his anonymity) or using electronic money with its informational consequences.

22. In promoting these principles, the drafters of the Recommendation have also sought to facilitate the free flow of data across frontiers. As will be seen from Principle 10 of the Recommendation, financial transactions are assuming a more transnational character. To avoid privacy based obstacles to the transfrontier exchange of personal data arising out of the use of a payment medium, it is hoped that respect for these principles in all the member States of the Council of Europe will provide an equivalent level of data protection for the personal data covered by this Recommendation. This principle goes hand in hand of course with the need to ratify the Data Protection Convention.

Operative part

23. The principles and guidelines contained in the Recommendation are addressed to the Governments of the member States. The Governments are invited to take these principles and guidelines into consideration in the context of such areas of law as banking law, consumer credit law, etc. The principles and guidelines may of course be taken up in the context of data protection law. It is not necessary to have recourse to binding legislation so as to take account of the principles and guidelines. Their respect could be ensured by means of codes of conduct or other self-regulatory measures adopted by bodies providing means of payment. There is an increasing trend towards self-regulation as a way of giving effect to data protection principles in certain sectors. Some major banks have already adopted codes of practice containing principles of good information management. It is felt, however, that codes of conduct and the like should be ratified by a superior organ, preferably the supervisory bodies set up under data protection legislation. With this in mind, bodies providing means of payment, as well as the beneficiaries of settlement operations and communication network operators should negotiate,

possibly through their representative associations where such exist, self-regulatory measures in consultation with the data protection authorities.

24. The text also invites the Governments of the member States to inform the competent data protection authorities, where such exist, of the existence of the Recommendation. It is believed that such authorities could use the sort of principles laid down in the Recommendation in settling disputes of a data protection nature which arise out of the provision and use of a means of payment. Bringing the Recommendation to the attention of the supervisory authorities, as well as to the principal actors named above, also provides all parties involved with a ready-made set of sound principles which could constitute the basis of a good and effective code of conduct.

25. Other international organisations are also dealing with issues relating to the provision and use of means of payment - for example, the Commission of the European Community, OECD and UNCITRAL. The texts under negotiation within these bodies are not primarily concerned with the data protection problems which arise in the area of means of payment. It is felt that the Governments of the member States in their dealings with such international bodies should direct the latter's attention to the special competence of the Council of Europe in the field of data protection and to the existence of this Recommendation and invite them to take account of the principles and guidelines contained in it.

APPENDIX TO RECOMMENDATION

1. Scope and definitions

26. As stated in the Preamble, the primary scope of the principles contained in this Recommendation concerns the automatic processing of personal data consequent upon ("linked to") the provision and use of a means of payment. It is of course the case that automatic data processing by bodies providing means of payment will be premised on various manual sub-processes - for example, the individual may fill in a short questionnaire giving details of his name, age, profession and sex. However, given the fact that these data will later be put on computer, it is only right that the principles contained in the Recommendation, in particular the principle of "fair and lawful collection" as reflected in Principle 3, apply to the manual sub-processing stages.

27. The references in the preceeding paragraph to manual sub- processes are not to be interpreted as giving rise to the assumption that personal data undergoing manual processing are included within the scope of the Recommendation. However, member States are of course at liberty to apply the principles contained in this Recommendation to personal data which are stored on manual media - for example, bank ledgers and card indexes. Such an approach is consistent with Article 3, paragraph 2 c. of the Data Protection Convention, and in fact certain member States do apply their data protection legislation to personal data undergoing manual processing. It is of course to be noted that manual processing is rapidly becoming a thing of the past, given the willingness and need of this sector to embrace new technology.

28. It is worth noting that manual data are to some extent protected by the principle of banking secrecy which applies to the communication stage irrespective of the processing medium. This point should be borne in mind in the context of Principle 5.

29. Principle 1.1, sub-paragraph 2, seeks to enumerate the various actors involved in this particular area. The text will occasionally at later stages provide specific principles in regard to each of them. It may be noted at this stage that bodies which provide means of payment may in fact be beneficiaries of transactions. For example, petrol companies may issue private label cards which can be used by individuals in point of sale terminals located in the premises of the various filling stations belonging to them. Similarly, it may be the case that the communications network operator, for example a PTT, may also profit from a settlement operation carried out by an individual, typically the payment of a telephone bill by means of a telebanking terminal.

30. The personal data which this Recommendation seeks to protect are defined in Principle 1.2. The definition proposed in Principle 1.2 is now well established and has been accepted without difficulty by the member Governments to which earlier sectoral recommendations on data protection have been addressed.

31. The Recommendation does not specifically include a reference to legal persons. Member States are of course free to apply the principles contained in the Recommendation to corporate bodies which, in the context of this instrument, could be the "beneficiaries". It is after all the case that bodies providing means of payment will store and process data on retailers, traders and service providers to whom the individual has transferred funds pursuant to a transaction.

Bodies providing means of payment may in addition store and process data relating to those undertakings which manage the use of a means of payment on their behalf. Accordingly, in those countries where the data protection regime includes legal persons, the principles contained in this Recommendation should accordingly extend to them. In those countries where legal persons are expressly excluded from the ambit of national data protection legislation, specific care should be taken in regard to those situations in which small traders, one-man companies, etc., are the recipients of a funds transfer operation, whether by cheque or by use of electronic media, and in regard to whom data are subsequently stored by the bodies issuing the means of payment. It may not always be easy to distinguish between personal data relating to individuals and data relating to corporate bodies, where the corporate body in question is to all intents and purposes an individual.

32. Given that the drafters of the text sought to concentrate on automatic data processing "linked to the provision of means of payment and of their use for payment or other related operations" (see Principle 1.1 supra), it is not surprising that a very broad definition of means of payment is provided in the text. In particular, it will be noted that the definition is not technology-specific; nor is it limited to means of payment which are issued in a physical sense - hence the text's insistence on "provision" rather than "issue" or "delivery" of means of payment. The definition put forward covers the various computerised, magnetic, electronic and telematic techniques which make it possible for funds to be exchanged without the need for paper - for example, chip cards, smart cards, magnetic stripe cards, automatic cash dispensers, telebanking, etc. However, the drafters were also anxious to take into consideration "non-electronic money".

It is for this reason that such matters as cheques and non-technology based cards are included within the scope of the Recommendation. Unlike a settlement operation by cash, a transaction carried out by means of a simple cheque or a non-technology based credit or debit card gives rise to informational value - for example the disclosure of the name and address of the bearer, as well as the time and location of the operation, to the beneficiary and subsequently to the bank. When these data are subsequently the subject of automatic data processing within the body issuing such means of payment, the drafters felt that they should fall squarely within the principles laid down within the Recommendation.

33. There are of course limits to the type of body covered by the expression "bodies issuing means of payment". It is only in so far as such bodies provide means of payment as defined above that they will be included in the definition. The bodies in question may be banking institutions in the strict sense of the term (and thus subject to principles of banking secrecy). On the other hand, they may be department stores issuing their own company-specific (private label) cards, building societies, petrol companies, car rental firms, etc. (and not subject to principles of banking secrecy). Given that the Recommendation only applies to bodies providing means of payment insofar as they provide a means of payment, it is not the intention of the drafters to include such bodies when they also provide investment services which may be provided at the same time as a transaction. For example it is now possible to transfer electronically the property in shares simultaneously with the payment for the investment transaction. The Recommendation is not concerned with the transfer of property, only with the system insofar as it is used for settling the payment.

34. In addition, the expression "bodies providing means of payment" is carefully defined so as to present a clear and accurate picture of what actually happens in practice in this sector. Any particular organisation may both provide a means of payment and manage the financial implications of its use. Alternatively, the management of the account may be placed in the hands of another body. For example, a department store may issue its own private label card and instruct a bank to take care of the day to day running of the clients' accounts. Furthermore, any particular organisation, banking or non-banking, may authorise another body to supply the means of payment to a client while undertaking itself to manage the account. All these different possibilities are envisaged in the definition of "bodies providing means of payment". The rights and duties of the bodies which receive instructions (contractors) to provide or manage means of payment on behalf of another undertaking will be governed by domestic law and determined by the contract.

35. The bodies referred to in the preceding paragraph may be of a private or public nature. As with the Data Protection Convention, data processing in either sector is covered.

36. So as to maintain consistency with related work being conducted within other international fora - principally the Commission of the European Community, OECD and UNCITRAL - the drafters of the Recommendation have not departed from the accepted definition of "communications network operator". The communications network operator may be of a public or private nature. This Recommendation is only concerned with the communications network operator insofar as he collects, stores and processes personal data. If his role is confined merely to providing the transmission link without engaging in the collection, storage and processing of personal data, he will only be bound by the principles concerning security of data (principle 8 of the Recommendation). It may be noted that there are already various international agreements which also address the need for communications network operators to ensure the security of their transmission systems. The communications link may also be leased from a general telecommunications network - for example, as in the case of the SWIFT system or in the case of interbank networks. This Recommendation is only concerned with the communications network operator in so far as he is in charge of operating a system. The principles will not apply to telecommunications authorities which merely provide software facilities. The operators of those facilities are, however, covered.

2. Respect for privacy

37. The drafters of the sectoral recommendations on data protection have customarily premised data protection principles on a general statement regarding the need to respect the privacy of the individual. This is felt to be a valuable exercise, serving as it does to indicate clearly the links between data protection and the private life of the individual, and that there are human rights issues at stake when personal information circulates within society as a whole or certain sectors of society. With this in mind, Principle 2 contains an exhaustive list of the various processing stages where privacy/data protection may be prejudiced. The text also calls the attention of the principle actors involved in this sector to the need to secure the confidentiality of personal data. The "necessary measures" referred to in the text will be the subject of greater discussion in the context of the principles relating to use of data and security of data.

3. Collection and storage of data

38. Articles 5.a and c of the Data Protection Convention posit respectively principles of fair and lawful data collection as well as storage limitation. How can such principles be given concrete meaning in the context of the collection and storage of personal data used for payment or other related operations, and embrace the different actors involved in this sector? Principle 3 of the Recommendation seeks to lay down a series of guidelines for bodies providing means of payment, communications network operators and beneficiaries on how data should be collected and stored.

39. Principle 3.1 takes up the storage of personal data by bodies providing means of payment. In brief, the data stored must be "necessary for making the means of payment available as well as the services linked to its use, including verification activities". In other words, to use the terminology of Article 5.c of the Data Protection Convention, the personal data stored must be adequate, relevant and not excessive in relation to those purposes. As regards the decision to provide a means of payment to an individual, the providing body may require information on for example, the name, age, address, sex, profession and salary of the applicant, and such other data as are necessary for the proper assessment of risks in making means of payment available. Bodies providing means of payment should avoid lengthy questionnaires which require information which is completely unrelated to the provision of a means of payment. As will be seen from Principle 3.3, the body providing the means of payment may need to evaluate the risks which it may run through provision of a means of payment to an applicant - for example, will the applicant run up large debts, will he abuse the means of payment by deliberately exceeding his credit limit? Checking on such risks ("verification activities") may require consultation with third parties and, as Principle 3.1 accepts, storage of the data collected.

40. The types of personal information referred to in Principle 3.1 may be termed a priori data. It is also the case that a posteriori data need to be collected so as to manage the account of the holder of the means of payment when he uses it for transactional purposes. It is the storage of such a posteriori data which is capable of producing problems of a data protection nature since the various uses of a means of payment by an individual may reveal certain aspects of his consumer preferences, location, movements, and even of his intimate life. Principle 3.1 stresses at this stage that only such data as are necessary for allowing the services linked to the use of a means of payment should be collected and stored. It will be seen that later sub-paragraphs of Principle 3 seek to place further limitations on the storage and use of personal data when the means of payment it being used.

41. The text accepts that bodies providing means of payment may sub-contract the collection, storage and processing of personal data to an agent. This is a normal feature of the means of payment sector. In accordance with Principle 3.2, the agent or "contractor" should be contractually bound to ensure that the data are not used for purposes other than those specified by the body providing the means of payment.

42. Principle 3.3 provides further guidance on how data may be collected fairly and lawfully by bodies providing means of payment. It is felt that the individual should be the primary source of information. It is accepted that sources other than the individual may be consulted with a view to deciding whether or not he is an appropriate person to receive a means of payment. The sort of sources in question may be publicly available information in the sense that the information is accessible to anyone - for example telephone directories and electoral lists. Consultation of publicly available files may help determine whether or not the individual

is who he says he is, whether his address is correct, whether he is habitually resident in the country, etc. Bodies providing means of payment may also wish to check on the solvency or credit worthiness of an applicant for a means of payment. For this purpose, they may have need to consult credit reference agencies or files containing lists of persons against whom judgement has been given in bankruptcy. Be this as it may, Principle 3.3 stresses the need not to exclude the individual from the information circuit. With the possible exception of publicly accessible sources of information, the individual should be fully informed about the possibility that third party sources may be consulted, the types of sources which may be consulted as well as the conditions under which such consultations may take place. He should be at liberty to withhold his consent to the consultation of certain sources. He may of course run certain risks if he does refuse to allow the body which he has approached about the issue of a means of payment to consult particular sources - the means of payment sought may not be provided. The individual should be clearly informed about the sort of risks which he may incur if he refuses to consent to the consultation of particular sources.

43. It may be the case that the body providing the means of payment will need to consult third party sources when the means of payment is being used by the individual. For example, if the individual is running up an overdraft, it may be necessary to consult a debt reporting agency to determine whether or not the individual is incurring financial liabilities in respect of other financial bodies. Once again, the individual should be clearly informed that the body providing the means of payment may in certain defined circumstances after provision of the means of payment check up on him by having recourse to third party sources.

44. While Principles 3.1 and 3.3 address the various bodies providing means of payment, Principle 3.4 concerns the beneficiary of a settlement operation. It imposes a strict storage limitation requirement. Retailers, traders and service providers will occasionally have to request the individual to provide proof of his identity so as to guarantee that he is the person entitled to use the means of payment. In addition, it may be necessary for beneficiaries to contact the individual's bank or other providing body with a view to determining his solvency. Retailers often keep lists of lost or stolen cards or cheque books which are circulated by issuing bodies, such lists may also specify the credit limits placed on the holder by the issuing body. Such lists may also be consulted by retailers since they are part of the process of validating payment. The collection and storage of data attendant on these controls are accepted. How long such data can be stored will be discussed in Principle 11. There is, however, no need for the beneficiary to retain a record of the precise nature of the transaction carried out by the individual in nominate form. For the purposes of such matters as legal action in the event of defective goods being bought or with a view to providing an after sales service, a simple anonymous receipt of the date and purchase is sufficient.

45. As noted in the discussion on "bodies providing means of payment", an organisation, rather than providing a means of payment, may limit itself to managing the account of a client supplied with a means of payment by another body. It may, for example, grant him overdraft facilities or provide him with a loan or extend to him some other financial service connected with the use of the means of payment. The provision of such services will be paid for by the body providing the means of payment. Accordingly, in many ways the organisation in question is to be regarded as a beneficiary and is subjected accordingly to the requirements of Principle 3.4.

46. When transactions are carried out by the individual using a means of payment - for example, electronic transfer of funds using a point of sale terminal, use of an electronic payment card in an automatic teller machine, or the purchase of goods and services via a credit card - certain details regarding the transaction must inevitably be communicated to the body providing the means of payment so as to allow the holder's account to be debited, and the beneficiary's account to be credited, or alternatively to move the holder's funds from one account to another account in accordance with the instructions given to the automatic teller machine or to a home banking terminal. Principle 3.5 imposes a storage limitation on such data. The data must only be stored to the extent required to validate and prove the individual's transaction as well as to carry out the services associated with the use of a payment medium, typically, moving funds from the individual's account to the beneficiary's account. There is no need for the body providing the means of payment to retain records which detail the nature of the transaction carried out by the individual using a means of payment, although it is inevitably the case that the necessary disclosure of the beneficiary's name and account number will indicate the sort of transaction which has been carried out. This principle obviously does not restrict the right of the holder of the means of payment to mention if he wishes the object of the transaction carried out; nor the need for the body providing the means of payment to carry out the object sought by the holder. Principle 3.5 also recognises that domestic law may require personal data to be collected and stored by bodies providing means of payment. By way of example, domestic law may require banks to keep a record of all fund transfers outside the jurisdiction which exceed a certain amount of money.

47. Although it is not expressly stated in Principle 3.5, it is considered acceptable for bodies providing means of payment to use credit scoring techniques to assess the level of risk in granting credit. Statistical models for risk evaluation are based on anonymous data. However, bodies providing means of payment may need to store personal data for a short period to enable them to be matched to risk models for the purpose of statistical prediction of risk in a particular case. It is felt that this limited, transitional period of storage of personal data is also acceptable.

48. Principles 3.1 to 3.5 are concerned with the need to avoid too much personal data being collected and stored by bodies providing means of payment and beneficiaries of settlement operations. It is by now well accepted that computer technology maximises the amount of personal data which can be collected, stored and processed. To reply to this concern, data protection policy lays down principles such as adequacy, relevance, non-excessiveness. However, technology itself may also provide technical solutions to minimise the amount of personal data which can be legitimately collected and stored. With this in mind, Principle 3.6 recommends that technical features should be integrated into, for example, electronic payment cards or hardware such as point of sale terminals or home banking terminals, with a view to ensuring that data which are irrelevant, unnecessary or excessive are not communicated to the body providing the means of payment or retained by the beneficiary.

49. Storage limitations are not only relevant to bodies providing means of payment and beneficiaries. The communications network operator defined in Principle 1.2, insofar as he collects, stores and processes personal data rather than merely providing the transmission link, must also be restrained in regard to the amount of personal data which can be stored. It is for this reason that Principle 3.7 is given over to delimiting the quantity of personal data which he

may collect and store, taking account of the functions which he performs in the means of payment sector.

50. Principle 3.8, second paragraph is quite clear on the issue of sensitive data of the types referred to in Article 6 of the Data Protection Convention, namely data revealing racial origin, political opinions or religious or other beliefs as well as personal data concerning health or sexual life. Such data must not be collected and stored. There is no justification for collecting and storing these types of sensitive data for the provision of a means of payment. It is however accepted that bodies providing means of payment will be anxious to know of the criminal past of an applicant for a means of payment. It is obviously against the interests of the body to provide a means of payment to a fraudster. The first sub-paragraph of Principle 3.8 only envisages bodies providing means of payment processing the criminal convictions of individuals where they are clearly relevant for determining whether or not the individual is a suitable person to be granted a means of payment. Recent offences relating to fraud and deception are clearly relevant. The processing is therefore justified unless it is otherwise possible to obtain relevant information for determining whether the individual should be granted a means of paymant. However, the processing of the applicant's road traffic offences is clearly not justified. They have no bearing on his suitability to be issued with or to continue using a means of payment.

51. However, even where the processing of criminal convictions is clearly justified, the processing of the data must satisfy the conditions laid down in Principle 3.8, sub-paragraph 1, namely the individual either must give his express and informed consent to their processing, or the processing must only be carried out in accordance with any safeguards laid down by domestic law.

4. Use of data

52. The rich nature of the personal information stored by bodies providing means of payment, as well as by beneficiaries, coupled with the multiplicity of the actors involved in the means of payment sector, has caused data protection specialists to reflect on the need to define clearly the legitimate purposes for which the information can be used. It is felt that the purposes specified in Principle 4.1 are a valid reflection of Article 5.b. of the Data Protection Convention insofar as bodies issuing means of payment collect and store personal data. For example, it is self-evident that the personal data stored by the body providing the means of payment can be used for the purposes of managing the account of the data subject - carrying out his instructions in regard to debiting or crediting his account, providing him with a statement so as to enable him to monitor his expenditure, etc. Bodies providing means of payment may also be obliged to take measures so as to avoid the means of payment being abused when it falls into the wrong hands, or if the bearer is habitually overdrawn as a result of exceeding his credit limit. With this in mind, Principle 4.1 recognises that bodies providing means of payment may use the data in these circumstances so as to minimise the abuse - for example, by circulating the name and account number of the bearer to banks or by circulating this information to traders and retailers in the form of a stoplist.

53. It will be noted that Principle 4.3 authorises the interconnection of different personal data files so as to enable the purposes outlined in Principle 4.1 to be accomplished.

54. One of the main privacy risks arising out of the provision and use of a means of payment is the possibility that when automatic data processing methods are brought to bear on the personal data created through use of a means of payment, profiles can be electronically constructed on individual behaviour, in particular spending habits and consumer preferences. These profiles have a commercial value. They may be used for targeting segments of the population by direct marketing firms so as to enable them to establish a marketplace in the individual's home by sending him information reflecting his taste in literature, holidays, household goods, and so on.

55. The drafters of this Recommendation have sought to impose limitations on the commercialisation or secondary use of a posteriori data as discussed earlier. With this in mind, Principles 4.2, 4.3 and 4.4 lay down guidelines for the protection of personal data which may be used for direct marketing or promotional purposes. It goes without saying that these guidelines are modelled closely on the principles laid down in the earlier recommendation of the Committee of Ministers in this area, namely Recommendation no. R (85) 20.

56. Principle 4.2 allows bodies providing means of payment to use the data stored by them to market and promote the various ranges of services, financial or otherwise, which they offer. The individual should be informed, and Principle 4.2 stresses that the information should be communicated in writing, that he may receive literature after a means of payment has been provided to him which will invite him to apply for such matters as savings schemes, investment services or other services of a non-financial nature (for example, travel) which the body offers. The written information should refer to the fact that the individual is not obliged to have his name placed on the providing body's mailing list. To determine whether an individual is a suitable person to receive a particular service (financial or otherwise), the body providing the means of payment may need to monitor the financial behaviour of the individual. Principle 4.3 authorises file interconnection for such purposes provided the individual has expressed his interest in receiving information on the various services offered by the providing body in accordance with the provisions of Principle 4.2. To deny a means of payment to an individual who informs a body providing a means of payment that he does not wish to receive marketing or promotional literature on the various services on offer would be unjust. It would be an exploitation of a superior bargaining position and would undermine completely the requirement to inform the individual in writing of his right not to appear on a mailing list (Principle 4.2, first sub- paragraph). In some European legal systems, such a situation may give rise to what is known as "abuse of rights". It is for this reason that Principle 4.2, sub-paragraph 2, envisages the individual being informed that his refusal to appear on the mailing list will in no way prejudice the decision to grant him a means of payment or to continue using it should he decide to withdraw his consent at a later stage.

57. Where the use of file interconnection or matching techniques are intended to draw conclusions on the individual which are not compatible with the purposes referred to in Principle 4.3, the body providing the means of payment must, unless authorised by domestic law, obtain the express and informed consent of the individual before linking up his various personal data files (Principle 4.3, second sub-paragraph).

58. It is the case that use of a means of payment will occasionally reveal certain sensitive data of the types referred to in Article 6 of the Data Protection Convention. For example, it may be possible for bodies providing means of payment to determine the political or religious views

of the individual when he instructs the bank to debit his account and credit the account of a political association or a religious institution. Standing orders in favour of certain clubs or societies may also reveal aspects of his sexual life. Principle 4.4 is quite clear on the use which can be made of such transactional data. The data may not be used for any purpose whatsoever, and certainly not for marketing or promotional purposes even if such purposes concern the provision of financial services.

59. Technology has now reached the stage where, among other things, electronic cards can be of a multifunctional nature. A smart card, for example, may be at the same time a means of payment and a portable medical file containing the medical history of the bearer, the treatment which he is receiving, and so on. Such a card may also be used as a means of access to secure premises. There are dangers in access being given to the financial data contained in the card's memory when it is being used for one of its other many functions. With this in mind, it is recommended that the card should be designed in such a way as to avoid access to the financial data stored in the memory when the holder is using it for a different purpose.

5. Communication of data

60. Frequent reference has been made in the commentary to the notion of banking secrecy which finds expression in the legal systems of the member States as a common law principle or as a provision in civil or penal codes, or even as a constitutional norm. As stated earlier, banking secrecy relates to the communication of personal data outside the framework of the banking institution (in the strict sense of the term) to third parties. While the various circumstances in which member States allow the veil of banking secrecy to be lifted are to a greater or lesser extent reflected in the provisions of Principle 5, it must be emphasised that Principle 5 is separate and independent from the rule of banking secrecy, and is concerned more with the situations which autorise use (communication of personal data for purposes other than those for which they were collected and stored). It should be noted that the principle of communication refers not only to the transfer of data to third parties who perform functions completely unrelated to the provision of financial services, but also to the subsidiary companies of bodies providing means of payment which engage in activities completely unrelated to the provision of means of payment. In other words, the communication of personal data by a body providing a means of payment within the same group will also be covered by the provisions of Principle 5 where the group is also composed of travel firms, insurance companies, etc.

61. Although not expressly stated in the text, member States could usefully reflect on the desirability of extending the principle of banking secrecy so as to include all bodies providing means of payment, and not just limit it to banks stricto sensu.

62. The following comments may be made on the sorts of situations referred to in Principle 5.1 (a) to Principle 5.1 (d):

- the "obligations laid down by domestic law" are not confined to statutory duties to communicate financial data to, for example, the tax authorities or the police. A court order may oblige a body providing a means of payment to disclose data, for example in the context of matrimonial proceedings involving the data subject and his/her spouse. An obligation may also arise where it is in

the public interest to reveal personal data for the purpose of crime prevention. It may be the case that a body providing a means of payment strongly suspects that illegally acquired funds are being laundered through it by an account holder. Such circumstances would justify the communication of the relevant data to the police;

- a body providing means of payment may need to protect its lawful interests by communicating data relating to a client who has been provided with a means of payment when it seeks to recover, in the context of legal proceedings, an outstanding debt which has been run up as a result of abusive over-spending by the client. The resolution of the litigation in favour of the plaintiff institution may require the client's transactions to be put before the court. It may also be the case that the body providing the means of payment will need to circulate a credit card number or the name of the bearer of a cheque so as to warn retailers, traders, etc., that the credit card or cheque is not to be accepted since it figures on a "stoplist". It should be noted that the interests of the body providing the means of payment which are at stake must be such as to clearly outweigh the privacy interests of the individual in non communication;

- the consent of the individual to the communication of his data by the body providing the means of payment to third parties must be "express and informed". Implied consent does not satisfy this requirement. Accordingly, should it be the case that bodies providing means of payment communicate, on a regular basis, information relating to the holders of bounced cheques to credit reference agencies, then the individual at the time of entering into the contract with an institution for the provision of a means of payment should be clearly forewarned of this possibility and should give his clear consent to it;

- some legal systems allow for the setting up of reporting or recording agencies which receive information from bodies providing means of payment relating to the fact that the holder of a means of payment is exceeding his credit limit and is, as a consequence, failing to honour the conditions governing the use of the means of payment. The text accepts that such a system may exist so as to increase payment security within the means of payment sector. In some ways, the provisions of Principle 5.1 (d) are closely related to those laid down in Principle 5.1 (b). It goes without saying that the data processing activities of the sort of body referred to in (d) are subject to the requirements laid down in domestic data protection legislation and in particular to the supervision of the control bodies instituted in accordance with such legislation.

63. As noted at an earlier stage in the commentary, bodies providing means of payment may sub-contract various aspects of their activities to third parties. For example, it may be the case that a company issuing a private label card will engage a bank to manage the account of the individual to whom the card is issued. Alternatively, a body providing a means of payment may hire out the data processing activities accompanying the issue and use of a means of payment. Or, the communications network operator may also have need of the personal data stored by the bank so as to enable the link to be made between the body providing means of

payment, the beneficiary and the data subject. Principle 5.2 of the Recommendation accepts that this sort of communication is in the normal course of things.

6. Publicity

64. Domestic data protection legislation typically requires data users to declare or register or notify in some other way their data processing activities with the competent supervisory authorities. In some cases, authorisation may be required before data processing can take place. Principle 6 reflects this situation. The factors outlined therein must normally be brought to the attention of the control bodies which in turn take steps to give publicity to the information which has been lodged with them. It is in this way that the individual is "informed about the existence of automated personal data files, their main purposes as well as the identity and habitual residence or principle place of business of the controller of the file" (Article 8.a of the Data Protection Convention). The desirability of rendering more transparent the data processing activities of bodies providing means of payment, beneficiaries and communications network operators insofar as the latter collect, store and process personal data can also be promoted by their own actions. There are practical ways of so doing. For example, the literature produced by the body providing the means of payment may be used as a vehicle to inform the individual of the sort of factors contained in Principle 6.

7. Right of access and rectification

65. If Principle 6 is viewed as a reflection of Article 8.a of the Convention, then Principle 7 is the concrete expression of Article 8.b and c.

66. It will be noted that no exceptions are made in regard to the sort of personal data which may be accessed by the data subject. It may, however, be the case that certain member States may restrict access to factual data, to the exclusion of subjective appreciations, opinions or evaluations on such matters as the credit risk of an individual. However, there is no reason in principle why the right of access should not extend to such data as well.

67. Principle 7.1 stresses the need for the data requested pursuant to exercise of the right of access to be delivered up in a form which the individual can understand. For this reason, the data should not be coded. They are, after all, his data and he should be able to appreciate their significance. Principle 7.1 also envisages allowing the individual to access personal data which are stored on the means of payment itself - in particular on magnetic stripe cards or microcircuit/chip/smart cards. For this purpose, the individual should be allowed access to an appropriate reader where possible, possibly under the supervision of the body providing such a means of payment, so as to allow him to see what is hidden from the naked eye. Where readers are not available, the individual should be able to receive the information in intelligible form; for example, from a print out of the data from his card to which he has a right of access according to national legislation. Once again, it is a question of his data and he should be entitled to have a genuine access to them.

68. The value of the right of access is shown in Principle 7.2. It gives the individual the right to ensure that the body issuing the means of payment is respecting the sort of principles laid down in the Recommendation.

69. There are practical ways of taking the "adequate measures" referred to in Principle 7.3 with a view to alerting the data subject to the fact that he has the rights laid down in Principle 7.1 and 7.2. The brochures and promotional literature produced by the financial institution or the statements which are issued by it on a regular basis to the client are useful ways of informing the individual of his rights of access, rectification and erasure, and how those rights may be exercised.

70. The intergovernmental Committee of experts on data protection which was responsible for elaborating the Data Protection Convention, as well as the earlier sectoral recommendations, has been anxious to ensure that the broad principles laid down in the Convention remain meaningful and effective in the face of technological evolution. The Committee has noted, inter alia, that data processing within organisations is no longer characterised by centralised storage and processing methods. There is now a trend towards networking and distributed data processing systems. Such decentralised data processing methods entail consequences for the rights of the data subject. For example, it may no longer be possible for the individual to have access to one single file containing the totality of the information held on him by certain organisations. Rather, a host of different files may exist. The Committee addressed this issue in its report "New technologies - a challenge to privacy protection?" which was adopted by the Committee of Ministers in 1988. The report recommends that a "logical" file should exist within organisations operating distributed data processing systems. Such a logical file would allow for ultimate location through retrieval methods of the personal data dispersed in the network. The drafters of the Recommendation have taken up this idea in Principle 7.4 so as to ensure that the individual can, to use the terminology of the Data Protection Convention, without excessive delay and without having to pay excessive subject access fees have access to the sum total of the information stored on him by a body providing a means of payment.

8. Security of data

71. Security of data is a key issue in a data protection policy. It is becoming increasingly important to reflect on ways of ensuring the integrity and confidentiality of personal data given the appearance of networking and distributed data processing systems. The circulation of personal information within this sector relies heavily on telecommunications links and networking. The guidelines laid down in Principle 8 apply to all parties engaged in settlement operations - the body providing the means of payment and processing the data accompanying its use, the beneficiary of the transaction, the technical operators managing the data transmission, the contractors (who may also be the technical operators) who may carry out certain processing operations on behalf of the providing body, as well as the PTTs which provide telecommunications links to allow such activities as home banking transactions to take place. As mentioned previously (paragraph 36), even though the communications network operator does not collect, store and process personal data, he should nevertheless be required to implement as far as possible the organisational and technical measures discussed below.

72. The appropriate organisational and technical measures referred to in Principle 8.1 should reflect the current state of the art. For example, use should be made of new coding and encryption techniques to safeguard the data when they are transiting through telecommunication links. The control measures referred to in Principle 8.2 may take various forms depending on the extent of involvement of the actor in data processing : access control to prevent unauthorised persons gaining access to computer systems processing personal data;

storage media control to prevent unauthorised reading of storage media; memory control to prevent unauthorised memory inputs as well as any unauthorised manipulation of stored personal data; access control to ensure that named authorised users of a data processing system can access no personal data other than those to which their access right refers; input control to ensure that it will be possible to check and verify at what times and by whom the various types of personal data have been processed; job control to ensure that personal data being processed by contractors or technical operators respect the conditions laid down by the issuing body; organisational control to ensure that the personnel of bodies providing means of payments, beneficiaries and as well as communications network operators are aware of data security measures and of the need to respect them, etc.

73. The individual himself has a role to play in data security. He should take the appropriate measures to ensure that his means of payment does not fall into the wrong hands or that third parties learn of his code number or PIN. The recommendation laid down in Principle 8.3 is already reflected in the practice of certain bodies providing means of payment. However, it is thought appropriate to recall the importance of the individual being instructed on the proper management of his means of payment and codes.

9. Remedies

74. The remedies referred to in Principle 9 may be contained in domestic legislation on data protection. The remedies may be supplemented by other guarantees laid down in civil, criminal or administrative law. In certain countries, the financial services sector is placed under the supervision of regulatory bodies or ombudsmen which allow the individual a means of redress against the activities of bodies providing a means of payment. It is essential, however, that such systems of supervision allow the individual to challenge the denial of the rights laid down in Principle 7, as well as to contest a breach of any of the other principles laid down in the Recommendation.

10. Transborder data flows

75. As noted in the Preamble to the Recommendation, payment or other related operations may have an international character. It is becoming increasingly the case that a means of payment issued in one country may be used in various other countries. At the same time, bodies providing means of payment may process abroad the data which they collect and store as a result of the use of a means of payment. Principle 10 of the Recommendation seeks to provide guidelines on how personal data may flow freely across borders without risk to individual privacy when such data arise from payment or related operations. The text distinguishes between flows of data between Contracting Parties to the Data Protection Convention (Principle 10.1) and flows of data between Contracting Parties and non-Contracting Parties (Principle 10.2).

76. As regards Contracting Parties, they participate in a common data protection zone by the fact of ratification and by having internal norms on data protection. In principle there should be no privacy-based obstacles to the circulation of data between and among such States. The integrity and confidentiality of the data collected and stored in the territory of one Contracting Party as a result of the use of a means of payment will be respected in the Contracting Party to which the data are subsequently transferred. This said, Article 12 of the Data Protection

Convention accepts the possibility that one Contracting Party may derogate from the principle of free flow where the regulations of the Party requesting the communication of the data do not provide equivalent protection for certain categories of personal data or of automated personal data files. The nature of the data in question will dictate the way in which this derogation operates. For example, the data may be of a sensitive nature. It may be the case for certain countries that banking data of a personal nature fall into this category. It is this sort of issue which is addressed in Principle 10.1 of the Recommendation. The drafters of the Recommendation felt that acceptance of the principles laid down in the Recommendation in all Contracting Parties could provide the necessary level of equivalent protection for personal data used for payment or related operations. "Equivalent" is not to be understood in the sense of identical. Respect for the principles contained in the Recommendation should be sufficient to provide an equivalent level of protection for the purpose of ensuring free flow of personal data used for payment or other related operations.

77. As regards the communication of personal data between a Contracting Party and a non-Contracting Party, the Recommendation encourages the competent authorities in a Contracting Party to ensure a free flow of data to other countries which respect the principles contained in this Recommendation. It will be recalled that there are countries which have data protection legislation but which have not yet ratified the Data Protection Convention. As regards such countries, respect for the principles contained in the Recommendation should, in the words of Principle 10.2, constitute "a strong justification for allowing personal data to be transferred to [them]". It is after all the case that the Convention is concerned with promoting transborder data flows, as well as protecting the private life of the individual.

11. Conservation of data

78. It is not in the interests of bodies providing means of payment, or beneficiaries, or communications network operators, to retain personal data when they have outlived their use. Principle 11.1 recommends that personal data should be kept no longer than is required for the performance of the various purposes referred to in Principles 3 and 4. The text also seeks to take account of the fact that it may be necessary to hold on data for a certain length of time for the purpose of defending legal actions or for furnishing proof of transactions carried out by the individual (Principle 11.3). For example, in some legal systems a use of a means of payment may give rise to a debtor-creditor-supplier relationship which allows the individual to sue the body providing the means of payment when goods purchased from a trader turn out to be defective. In such cases, it is obviously necessary for the body providing the means of payment to retain an account of the transaction. However, such data should only be stored for a reasonable period. It is with this in mind that Principle 11.3 of the Recommendation encourages bodies providing a means of payment to draw up time limits for the conservation of data.

79. Principle 11.3 also addresses the issue of what should happen to personal data furnished by an individual in the hope of being granted a means of payment and who is subsequently refused. In these circumstances, it may be the case that the individual may seek to challenge the decision - for example, on the basis that he/she was refused the means of payment on sexual or racial grounds. It will be necessary for the body to have a record of the negotiations with the aggrieved individual so as to allow it to defend the action. However, and once again,

the data are not to be retained indefinitely. Time limits should be laid down for the conservation of personal data once a means of payment has been refused.

80. Principle 11.2 of the Recommendation takes up the issue of the role of the contractor processing data on the instructions of a body providing a means of payment. In brief, once the contractor has discharged his duties, any personal data in his custody should be deleted.

12. Ensuring respect for the principles

81. The system of supervision referred to in Principle 12.1 could be constituted by the control bodies set up by virtue of national data protection legislation. The registration/declaration/authorisation requirements which such legislation may impose on data users could promote the desired transparency for bodies providing means of payment which is recommended in Principle 12.2. Respect for the principles contained in the Recommendation could be promoted by data protection authorities in conjunction with representative associations of bodies providing means of payment. To ensure respect for the principles, such representative associations could enter into a dialogue with the supervisory authorities with a view to elaborating codes of conduct for the protection of personal data in the area of means of payment and related operations.

82. As stated at an earlier stage of the memorandum, it is often the case that bodies providing means of payment are subject to control by regulatory bodies or ombudsmen for the financial services sector. It is believed that these sorts of institutions may also have a valuable role to play in promoting respect for data protection, and in particular the sort of principles contained in this Recommendation, within the sector.