COUNCIL OF EUROPE
COMMITTEE OF MINISTERS

RECOMMENDATION No. R (90) 19

OF THE COMMITTEE OF MINISTERS TO MEMBER STATES

ON THE PROTECTION OF PERSONAL DATA USED FOR PAYMENT AND OTHER RELATED OPERATIONS[1]

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

The Committee of Ministers, under the terms of Article 15.*b* of the Statute of the Council of Europe,

Considering that the aim of the Council of Europe is to achieve a greater unity between its members;

Aware of the increasing use of automated data processing in the area of means of payment and other related operations, and the advantages to be gained;

Aware of the increasing use of automated data processing by bodies providing financial services, some of which are not necessarily banks;

Believing that the use of automated data processing in the area of means of payment and other related operations may entail risks to the privacy of the individual;

Believing moreover that, notwithstanding the increasing use of automated data processing in the area of means of payment and other related operations, individuals should not be compelled to make use of electronic means of payment, so allowing them the possibility of keeping to a minimum the amount of personal data which is disclosed in the course of transactions;

Recognising that the provisions of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data of 28 January 1981 apply to the automated data-processing activities of bodies providing financial services;

Believing, however, that it is appropriate to apply the general provisions of the convention more specifically so as to adapt them to the particular requirements of the types of operations referred to above;

Bearing in mind the international character of certain of these operations and the transborder flows of personal data to which they give rise, which make it necessary to promote an equivalent level of data protection in all the member states of the Council of Europe,

Recommends that the governments of member states:

— take account in their domestic law and practice in the area of means of payment and other related operations of the principles and guidelines appended to this recommendation;

---

1. When this recommendation was adopted, the Representative of the United Kingdom, in application of Article 10.2.*c* of the Rules of Procedure for meetings of the Ministers' Deputies, reserved the right of his government to comply or not with the following paragraphs of the appendix to the recommendation: 3.3, 3.4, 5.1.*c* and 7.1.

— bring this recommendation to the attention of the competent authorities in the field of data protection as well as to the attention of bodies providing means of payment, beneficiaries and communications network operators or their representatives.

Appendix to Recommendation No. R (90) 19

1. *Scope and definitions*

1.1. The principles contained in this recommendation apply to the automated processing of personal data linked to the provision of means of payment and of their use for payment or other related operations.

In addition, these principles apply to all parties involved in those operations (beneficiaries, bodies providing means of payment and communications network operators).

1.2. For the purposes of this recommendation:

The expression "personal data" covers any information relating to an identified or identifiable individual. An individual shall not be regarded as "identifiable" if identification requires an unreasonable amount of time, cost and manpower.

The expression "means of payment" covers all payment instruments and other means used for payment orders, in particular cheques, giro orders and payment cards as well as all other types of debit orders and credit orders whether or not initiated by an electronic signal.

The expression "beneficiary" includes all legal and natural persons who benefit from payment or other related operations, and in particular traders, retailers and service providers to the exclusion of the individual consumer.

The expression "bodies providing means of payment" covers all banking and non-banking undertakings which provide or manage means of payment whether regularly or intermittently.

Undertakings which receive instructions from the main providing body to provide or manage means of payment are also covered.

The expression "communications network operator" refers to the body which provides the transmission for processing the data which are used to carry out the payment or other related operation.

2. *Respect for privacy*

Respect for privacy shall be secured during the collection, storage, use, communication and conservation of personal data linked to the provision or use of a means of payment. For that purpose, bodies providing means of payment, beneficiaries and communications network operators shall take the measures necessary to secure the confidentiality of those personal data.

3. *Collection and storage of data*

3.1. With regard to the provision of a means of payment, personal data should only be collected and stored by the body providing the means of payment in so far as such data are necessary for making the means of payment available as well as the services linked to its use, including verification activities.

3.2. In accordance with provisions of domestic law, the body providing a means of payment should be able to entrust the collection, storage and processing of these data to a contractor in so far as the latter undertakes not to use the data for other purposes.

3.3. In principle, personal data should only be collected from the individual concerned. Where other sources need to be consulted, the individual should, prior to consultation, be fully informed about the categories of sources which may be consulted, as well as the consequences attaching to a refusal or withdrawal of consent.

3.4. Personal data may only be collected and stored by the beneficiary for the purposes of verifying the identity of the holder of the means of payment and for the determination of the validity and lawful nature of the payment or other related operation.

3.5. When an operation is carried out with a means of payment, the personal data relating to this operation should only be collected and stored by bodies providing means of payment to the extent necessary for validation and proof of the operation as well as for carrying out the services and fulfilment of any obligation laid down by domestic law associated with its use.

3.6. Payment systems should be designed in such a way as to avoid, in the course of a payment or other related operation, personal data which are not necessary for the accomplishment of the purposes set out in principles 3.1 and 3.5 respectively being communicated to the body providing the means of payment and personal data which are not necessary for the accomplishment of the purposes set out in principle 3.4 being retained by the beneficiary.

3.7. The communications network operator should be able to collect and store only those personal data which are necessary for carrying out the services which he provides, or which are necessary for the purposes of proof and billing of such services.

3.8. The processing of personal data relating to the criminal convictions of an individual should only be carried out where the data are of such a nature that they are clearly justified for determining the suitability of that individual for receipt or continued use of a means of payment, and provided the individual has given his express and informed consent or the processing is in accordance with safeguards laid down by domestic law.

The collection and storage of the other categories of sensitive data referred to in Article 6 of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data should not be permissible.

4. *Use of data*

4.1. Subject to the provisions of principle 4.2, personal data collected and stored in accordance with principle 3 should only be used to determine whether a means of payment should be provided to an applicant, for verification purposes, for managing the account concerned, including the provision of statements, or to avoid abuse in the case of loss or withdrawal of the means of payment.

4.2. Provided the individual has been fully informed in writing and unless he has objected, the body providing the means of payment may use the data collected and stored for the purposes referred to in principles 3.1 and 3.5 for marketing and promoting its range of services with regard to him.

The individual should be informed of the fact that, if he objects to his data being used for marketing and promotional purposes, this will not prejudice the decision to provide him with a means of payment or to allow him to continue using a means of payment already issued.

4.3. The interconnection of different personal data files resulting from the various uses of a means of payment by the individual should only be carried out by the body providing the means of payment for the purposes referred to in principle 4.1 or for the marketing and making available of services which the individual has accepted in accordance with principle 4.2.

Unless otherwise provided by domestic law, or with the express and informed consent of the individual, the interconnection of different personal data files for purposes other than those referred to in this principle should not be permissible.

4.4. To the extent that the use of a means of payment gives rise to sensitive data, such data may not be used for marketing, promotion or any other purposes.

4.5. If a multifunctional card is also, among other things, a means of payment and is used for purposes other than those referred to in principle 1.2, second sub-paragraph, it should be designed in such a way as to make access impossible to the type of personal data covered by this recommendation when it is being used for such other purposes.

5. *Communication of data*

5.1. Personal data collected and stored for the purposes referred to in principles 3.1 and 4.1 may only be communicated in the following cases:

a. in accordance with obligations laid down by domestic law;

b. when it is necessary to protect the essential and legitimate interests of the body providing the means of payment;

c. with the express and informed consent of the individual;

d. in case of a default in payment, where a system of reporting or recording of such information has been set up in accordance with domestic law to increase payment security within the sector covered by this recommendation;

5.2. The conditions laid down in principle 5.1 shall not restrict the communication of personal data by the body providing the means of payment to contractors acting on its behalf or to the communications network operator in so far as communication is necessary for the issue and use of the means of payment.

6. *Publicity*

In accordance with domestic law and practice, bodies providing means of payment, as well as beneficiaries and communications network operators, should ensure that the individual is informed about the nature of data which they store, the purposes for which the data are stored, the categories of persons or bodies to whom the data may be communicated and the legal basis for such communication.

7. *Rights of access and rectification*

7.1. Each individual should, on request, be able to obtain all data concerning him in an intelligible form, such data as are contained on a means of payment.

7.2. He should be able to have such data rectified or erased where they are found to be inaccurate, irrelevant, excessive or have been collected or stored in disregard of the principles set out in this recommendation.

7.3. Bodies providing a means of payment should take adequate measures so as to ensure that the data subject is aware of his rights in regard to his data as laid down in principles 7.1 and 7.2, as well as the ways and means of exercising them.

7.4. The body providing means of payment should ensure that the data subject can, without unreasonable delay or expense, exercise his right of access, in particular where a system of distributed data processing involves the location of his data on several files.

8. *Security of data*

8.1. Each party to the payment or other related operation should take appropriate organisational and technical measures so as to safeguard the security, integrity and confidentiality of personal data against unauthorised access, use, communication, alteration or distortion.

8.2. Control measures which are sufficient to guarantee the protection of the data should be provided for by beneficiaries, bodies providing means of payment and communications network operators.

In particular, the latter should inform their staff of such measures and of the need to respect them. Measures should be taken within the organisation so as to designate by name those members of the staff who are entitled to have access to the data.

8.3. Bodies providing means of payment should give their customers advice regarding security, including advice on how to manage and keep means of payment and codes safe, and the procedures to be followed in case of loss or theft of a means of payment.

9. *Remedies*

Domestic law should provide a remedy in cases of breach of the principles laid down in this recommendation, in particular where the rights laid down in principle 7 are not respected.

10. *Transborder data flows*

10.1. Where the provision or use of a means of payment requires the collection, storage or processing of certain personal data in two or more Parties to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, no obstacle should be created for the transborder flow of such data between and among them provided the principle of equivalent protection is guaranteed.

10.2. If the state to which the data are to be transferred is not a Party to the convention, respect for the principles contained in this recommendation in that state shall be regarded by the competent authorities in the Contracting Parties as a strong justification for allowing personal data to be transferred to that state.

11. *Conservation of data*

11.1. Where personal data are no longer necessary for the accomplishment of the purposes referred to in this recommendation, they should be deleted.

11.2. Contractors responsible for processing data on behalf of bodies providing means of payment should not retain them beyond the period necessary for carrying out the instructions received.

11.3. Consideration should be given to the desirability of providing time-limits for the conservation of personal data once a means of payment has been refused. Time-limits should also be set which take into account such matters as the need to retain data for the period necessary for the purpose of defending legal actions or for furnishing proof of transactions carried out by the individual.

12. *Ensuring respect for the principles*

12.1. Each state should institute a system of supervision making it possible to secure respect for the principles set out in this recommendation.

12.2. For this purpose, each state should ensure that all bodies providing means of payment are easily identifiable.