**Guiding principles for the protection of personal data with regard to smart cards (2004)**

**As adopted by the CDCJ at its 79th Plenary (11-14 May 2004)**

## INTRODUCTION

The Council of Europe's data protection committees wished to draw attention to certain specific aspects of the protection of personal data with regard to the use of smart cards. The Project Group on Data Protection (CJ-PD) of the Council of Europe therefore requested a consultant, Mr Karel NEUWIRT (President of the Czech Data Protection Authority), to write a report on data protection with regard to the use of smart cards. This Report acknowledged that any study on smart cards would be linked to technological developments and should thus be situated in the historical context. The wish was therefore expressed to draw up a list of specific Guiding Principles to be taken into account in relation to the use of smart cards.

After examining Mr Neuwirt's report and guiding principles, the CJ-PD agreed to revise and specify some of these guiding principles, and prepared the following text.

For the purposes of these guiding principles, a "smart card" is thought of as a mobile carrier of personal data with automatic processing functions, which is issued to the data subject and processes personal data in accordance with the purposes and specifications of the issuer in connection with an information system related to it. The card can be used, for example, for the purposes of identifying the data subject, concluding transactions that cannot be done anonymously or allowing access to certain places and databases. A smart card should be distinguished from a magnetic strip or a memory card, which cannot be used for autonomous logical and arithmetical operations with data.

Smart cards are increasingly used for various applications. The nature and capability of smart cards create many data protection issues and these new problems need to be addressed, for example who controls the personal data used in the system? Who is responsible for the accuracy and security of the data when the system is accessible to a number of other entities? How can the multiplication of risks of the possible invasion of the privacy of citizens due to the use of smart card technology be countered? Who has access to the data subject's personal data and under what conditions? etc.

Information systems which use smart cards entailing the processing of personal data fall within the scope of application of the Council of Europe Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data [ETS No.108] (hereinafter Convention 108). This Convention was prepared when it became apparent that in order to ensure the effective legal protection of personal data it would be necessary to develop more specifically and systematically the general reference to respect for private life in Article 8 of the Convention for the Protection of Human Rights and Fundamental Freedoms (hereinafter ECHR).

Additional rights and safeguards are laid down in various Council of Europe recommendations, in particular:

a) Recommendation No. R (2002) 9 on the protection of personal data collected and processed for insurance purposes
b) Recommendation No. R (99) 14 on universal community service concerning new communication and information services
c) Recommendation No. R (99) 5 for the protection of privacy on the Internet
d) Recommendation No. R (97) 5 on the protection of medical data
e) Recommendation No. R (95) 4 on the protection of personal data in the area of telecommunication services, with particular reference to telephone services
f) Recommendation No. R (90) 19 on the protection of personal data used for payment and other related operations
g) Recommendation No. R (89) 2 on the protection of personal data used for employment purposes
h) Recommendation No. R (86) 1 on the protection of personal data used for social security purposes
i) Recommendation No. R (85) 20 on the protection of personal data used for the purposes of direct marketing

A number of activities and instruments of the Council of Europe, in particular the work of its expert committees concerned with personal data protection, indirectly relate to the issues raised by the use of smart cards. In particular, as smart cards may be used as a storage medium for biometric data, attention is drawn to the guiding principles on the protection of personal data in the form of biometric data, currently being prepared by the T-PD. Modern technology brings a number of advantages to the daily lives of citizens, as well as risks due to the possibility of interfering in the privacy of individuals. It is not, therefore, the objective of this Council of Europe document to describe the advantages of using smart cards, but to specify the approach that should be followed in order to improve personal data protection when smart card technology is used.

Collecting and processing personal data in systems which use smart cards should respect all the principles of personal data protection established by national legislation.

The following guiding principles are not intended to be an exhaustive solution to all the data protection issues arising with respect to the use of smart cards. A smart card is always used as part of a wider information system and the overall effective protection of personal data used in such a system depends on many different factors and circumstances. The security of a system also greatly depends on the behaviour of the people who come into contact with it. Smart card technology is undergoing very rapid development. These guiding principles are intended to set out basic principles that will not significantly change with innovations in the technology. Nevertheless, it may be appropriate to supplement these principles in the light of the continuing developments in this field.

It should be recalled that, to the extent that these guiding principles contain safeguards for everyone's rights and fundamental freedoms, and in particular the right to the respect for privacy, as established by Articles 5, 6 and 8 of Convention 108 and Article 8 of the ECHR, derogations from such rights, in accordance with Article 9 of Convention 108, which was elaborated on the

basis of Article 8 of the ECHR, are possible where they are provided for by law and constitute a necessary measure in a democratic society in the interests of:

a. protecting State security, public safety, the monetary interests of the State, or the suppression of criminal offences;

b. protecting the data subject or the rights and freedoms of others.

In relation to these derogations, it might be underlined that they should be interpreted in a restrictive manner and they should be used only in exceptional cases in accordance with the interpretation of paragraph 2 of Article 8 of the ECHR in the case law of the European Court of Human Rights.

The guiding principles are primarily aimed at the issuer of the card, who holds primary responsibility for the protection of personal data contained on the card. They are also directed at all other participants involved in information systems – project designers, managers, operators, as well as the data subjects themselves – who should take these principles into account. The principles that have been laid out should be applied as consistently as possible. Only thus will it be possible to contribute to the rise of internationally interoperable and highly secure smart card applications.

## GUIDING PRINCIPLES

1. The collection and processing of personal data by means of smart cards should be fair and lawful. Only the personal data necessary for the fulfilment of the purposes for which the card is used should be collected and stored on the card. Systems using smart cards should be transparent[1] to the data subjects whose personal data are processed.

2. Personal data should only be collected and stored on a smart card for legitimate, specific and explicit purposes. They should not be used subsequently in a way which is incompatible with these purposes.

3. The obligations with regard to the protection of personal data fall upon the person who determines the purpose of the system and the means that are used to fulfil this purpose. This implies, in the case of a multipurpose card, that different controllers are each responsible for their part.

4. If a smart cart is used for different purposes, the processing should be organised in such a way that the data are not used for purposes other than those for which they were collected. When the same data are used for several purposes they should be limited to what is strictly necessary.[2]

[1] This notion of transparency implies that the data subject is informed about the data that are stored and the use that is made of them.

[2] For example, in the case of a smart card used by a school in both at the cafeteria and the library, only the data commun to these two purposes, such as the name of the child and his or her class, should be stored.

5. Sensitive personal data[3] to be recorded in the card's memory should only be collected if provided for by law or if the data subject has given his/her explicit consent[4]. These data should only be processed in accordance with appropriate safeguards laid down by law.[5] If the collection and processing of such data are based on explicit consent, the data subject should have the right to withdraw consent at any time. Refusal or withdrawal of consent should not be sanctioned with any negative consequences for the data subject. [6]

6. Data recorded on a card should be protected against any unauthorised or accidental access, alteration and/or erasure. The card should offer an appropriate level of security given the state of technology, the sensitive or non-sensitive nature of the data recorded, the number and type of applications and the evaluation of possible risks.[7] The conditions under which third parties may have access to data recorded on the card should be established beforehand for each of the separate purposes for which the card is used.[8]

7. Where personal data are collected and stored on a smart card, the data subject should be informed of the purposes of processing, the identity of the controller, the categories of data concerned and the recipients or categories of recipients of the data that are stored. Other information[9] should be provided to the data subject, where this is necessary to guarantee fair processing of personal data.

8. When a card is issued, the holder should be properly informed about how to use his/her card and what to do in case of fraud or unauthorised disclosure[10].

9. Whenever personal data are exchanged between a smart card and the system, the data subject should be alerted, unless he/she already has this information. This is particularly important in the case of contact-less cards, that is to say if the data subject does not insert or present the card to the system him-/herself.

---

[3] According to Article 6 of Convention 108, sensitive personal data include "personal data revealing racial origin, political opinions or religious or other beliefs, as well as personal data concerning health or sexual life [...] [and] personal data relating to criminal convictions". Other data defined as such in national law are also considered as sensitive data.

[4] However, there may be cases in which national law provides that consent is not a sufficient basis for the lawfulness of collection or processing.

5 Such appropriate safeguards providing additional protection for the data can be implemented, for instance, by encryption of data, which is the most sophisticated device at present. Account should be taken, however, of possible future technical developments.

[6] If the recording of sensitive personal data is necessary to provide the data subject with a service, and he or she refuses to give explicit consent or withdraws consent, the service will of course no longer be available to him or her.

[7] If, for example, cards with a memory chip are used, in principle only personal identification data may be recorded. There may also be other criteria which should be taken into account, such as quantity of data, the number of potential readers, the purposes of processing, etc.

[8] The risk of the data stored on the card being misused increases when it is equipped with payment functions. Combining the payment function of the card with applications through which the cardholder's sensitive personal data are recorded on the card is not recommended.

[9] The information to be provided to the data subject may also include technical specifications of the system chosen.

[10] In particular, the attention of the holder of the card should be drawn to the consequences that may result from misuse of the card, disclosure of the way to access data (for example the code) or disclosure of the data, and to the fact that his/her liability may be engaged in some cases.

10. Data subjects should have the right of access to personal data relating to them contained on the card and should have the right to have them corrected or, where necessary**,** updated[11].

11. Data resulting from the use of a smart card[12] should be deleted if they are no longer necessary for the specific purpose for which the card was used.

[11] One way of guaranteeing access is by setting up card readers

[12] An example of such data is data giving information about the date and place when the card was used.