Open Smart Card Infrastructure for Europe

v2

Volume 2: **User Requirements**

Part 2: **General model for a Privacy Code of conduct for interoperable smart card systems**

Authors: **Expert Report for eESC TB8 User Requirements**

PREPARED BY: JAN HOLVAST

DOCUMENT HISTORY

Name/function	Action	Circulation	Version
Jan Holvast Jan van Arkel	Initial Draft	Internal	v. 0.1
Henry Ryan	English Review	External	v. 0.1-1
Jan Holvast	Second Draft	Internal	v. 0.2
Jan Holvast Jan van Arkel	Final Draft	External	v 1.0

For further information please contact any of the following persons:
Jan Holvast henp.holvast@planet.nl
Jan van Arkel arkel@cardlife.nl

Table of contents

General Explanation

1. Introduction

Smart cards by definition are capable of storing and processing data. In many cases this concerns personal data i.e. any information relating to an identified or identifiable natural person. While smart cards are a ubiquitous technology which may be applied in many different ways, the most crucial requirement is perhaps the level of its acceptance and adoption by the European citizen, the end-user. In order to stimulate the social acceptance of the cards and to promote their harmonised introduction, the eESC constituency has therefore agreed on the general conditions to ensure personal data protection. These conditions which are derived from the European Directive 95/46/EC are elaborated and laid down in this General model for a Privacy Code of conduct for interoperable smart card systems.

2. Privacy

Privacy can be described as the right to self-determination -within certain limits- of one's own environment, one's own body and one's own data. Of the three spheres mentioned (environment, body, data), the Rules of Conduct are limited to determination of information on data. The following Rules therefore refer to informational privacy: privacy with regard to all aspects of the information operation process.
The following aspects are concerned:
• data collection or observation
• data entry
• data storage
• data operation
• data disclosure or use.

The reservation `within certain limits' indicates that this right to self-determination must always be weighed up against other interests: e.g. public interest, economic interests (including the interest of smart card issuers, and service providers), the interest of medical and scientific research, interests of other people. In most cases lack of informational privacy will not cause problems, because it is clear that in certain cases the right to self-determination must yield to other more important social or general economic interests.

3. General principles of data protection

Sometimes restriction evokes resistance. For example, a data subject may resist when he is of the opinion that an unwarranted restriction has been made or that he has not been informed sufficiently about the specific reasons for the restriction.
An additional problem of the information operation process is that the separation between the collection or observation of data and their final use can sometimes be so great that the individual loses sight of this process and feels he no longer has control over his own personal data.

Two criteria are important in the discussion on personal data. The first is that the information must be related to a natural person, the second is that the person must be identifiable. “Related to a natural person” does not mean that under all conditions data on objects is not or cannot

become personal data. The way in which the data are qualifying a person in the social context is the decisive factor. For instance, a combination of data on cars, houses and small companies are treated as personal data, ~~when it can be used to identify an individual~~ while they are qualifying not only objects but also the persons that possess these objects. For being identifiable, direct identifiable characteristics are not the only means of identification. A combination of indirect characteristics, without any name or address can by combination be used to precisely identify a particular individual. .

The first prerequisite of the Rules of Conduct with regard to better protection of privacy is the principle of openness: all aspects of the information operation process should be transparent to the cardholder. Only then can the cardholder understand why data are needed in certain situations, why his privacy cannot remain 100% uninvaded and what freedom of choice he himself has in this.

The Rules pay special attention to three aspects of the information operation process. This is due to the fact that these, more than other aspects, are related to the right to self-determination:

- data collection or observation
- data storage
- data use

Data collection
With regard to data collection or observation the Rules of Conduct observe that mankind can or must leave traces in most of his activities.
Some of these traces are so important that they are processed in the form of personal data: medical data, purchasing behaviour, information supplied when applying for services. From the point of view of the cardholder, the **recognizability principle** is important, that is to say that only data may be collected which have been obtained lawfully and for which the cardholder has given permission or at least knows that these data are being collected and for which purpose this collection takes place.

Data storage
Two problems may occur in the storage of data. The first is that of data pollution: sometimes personal data are stored which are incorrect, incomplete, inaccurate or irrelevant. The second problem is that of unauthorized access to the data that have been stored e.g. inadequate protection against hacking, managing data carelessly so that anybody can consult or alter them.

In order to prevent these two problems, a **carefulness principle** is necessary, consisting of three aspects. These imply:

- that the data should be checked for correctness, completeness, relevance and topicality;
- that the cardholder has the right to consult his own data and, if necessary, to correct them;
- that technical and organizational measures should be taken against unauthorized forms of use, disclosure, alteration or destruction of the data.

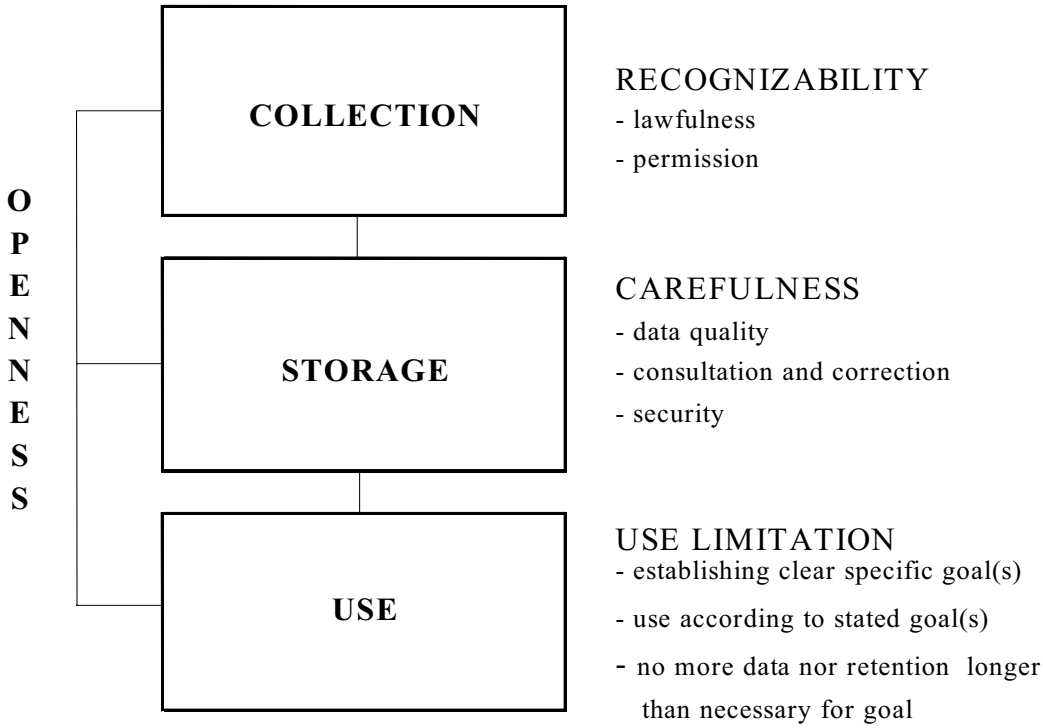

Figure 1: Privacy Principles

Data use

From the point of view of the right to self-determination the main issue for "data use" is the risk that data are used for purposes other than the one for which they were originally and validly collected. For example, the potential linking of separate databases and using data so derived to target specific individuals for unauthorised ends, can be a cause for concern. In order to prevent this danger, the **use limitation principle** is maintained. This principle has four aspects:

- the purpose for which the data are collected and further processed should be laid down and be (made) known to the cardholder from the beginning;
- use and disclosure of data should take place in a way compatible with the purposes for which they are collected, unless it concerns a legal obligation to disclosure or else disclosure or use with explicit consent of the data subject;
- only adequate, relevant and not excessive data should be stored;
- data should not be kept longer than necessary for the purposes for which the are collected or for which they are further processed.

4. Privacy and smart cards

In the Rules of Conduct these general principles are applied to smart cards. Smart cards have many applications and are applied in many sectors. One of the most promising application is the IAS, the set of processes, data and technology agreements required in a given environment to provide Identification, Authentication and Signature Services. For this reason a Framework IAS is formulated who's aim is to facilitate interoperability between the various IAS-schemes throughout the world. The use of a public Electronic Identity, combining private-public keys and corresponding public key certificates, is an example of this development. As a

preliminary observation it is noted that the use of smart cards provides a way of both increasing and decreasing transparency. In addition just like the computer in its initial phase, there is something magical, something mysterious about the smart card. A card the size of a credit card is capable of collecting, storing and modifying data, and with the help of other equipment these data can be electronically transferred. In short a smart card can be viewed as a pocket-size computer.
The smart card offers possibilities to increase the transparency of the data operation process. By use of convenient card reader terminals the card user can view their own data (including data for identification, authentication and for a digital signature) in a relatively simple way. and possibly also view the data in the related registers of personal data.
Ready access to information, on these and other aspects of the information operation process, can help provide a much needed prerequisite for increasing the consumer's willingness for acceptance.

With regard to the three aspects of the information operation process mentioned above, a smart card can be the ultimate instrument for tracking individuals and transferring data on their activities to cumulated registers of personal data e.g. purchasing behaviour in shops, use of motorways, use of medicines. Naturally, in many cases collecting or observing these data is often also to the advantage of the cardholder, but it is important to make it absolutely clear beforehand what data are collected on which occasion. This is especially an issue when contactless cards can in some cases be read and updated from a distance without requiring direct action from the cardholder or even without the cardholder knowing.

The set of agreements cannot provide an unambiguous answer to the question of how many and what data should be recorded on the card itself. This depends on the application and the functions that are used. In some cases only identifying data are recorded on the card, whereas in other cases an abundance of other data is recorded. In both cases data can be incorporated in related databases.

From a privacy point of view, data use is the most crucial aspect of the smart card. The starting principle is use limitation. However, it is necessary to prevent card issuers and application providers from (tacitly or not) expanding the number of objectives of the card in an unlimited and uncontrolled way. This possibility does exist, especially for a multi-application and multi-service cards.
Another point needed special attention is profiling. If no arrangements are made against this, it is possible to easily compile an individual blueprint of the cardholder for a multi-application card with many `user' data. All the person's data are then brought together: payments, medical data, other supported activities.
The card can also stimulate the possibilities of linking if a common feature, for instance a personal registration number (if the use of that common number is legally permitted) is incorporated in several otherwise independent registers of personal data. In this case the card can also be used to rapidly verify data in the relevant databases.
These forms of use evoke the greatest cardholder fear of invasion of privacy. The Rules of Conduct therefore provide a set of agreements within a smart card community that prevent uncontrolled and undesired use of personal data by card issuers and application providers. (See also GIF Part 1 and Part 2 documents). This is put into effect through a system of compartmentalization whereby individual application providers each acquire their own independent area or compartment of the electronic memory of the smart card. Every application provider has exclusive reading, writing and data operation authority for only his

own field of application. Every application does have the possibility to consult and use but not to modify the general personal data recorded on the card by the card issuer. These separated responsibilities and possibilities for use are designed to remove the fear of data intentional or accidental misuse of personal data.

5. Privacy Rules of Conduct

All three principles mentioned above are an integral part of any implementation of European Directive 95/46/EC and thus by definition also part of the national legislation in the Member States, based on this Directive, which aim to protect privacy in storing and using personal data.
The construction of a code of conduct is strongly supported by the Directive.
The objective of such a code for Smart Cards is that:
• specific measures are taken for certain defined circumstances
• future developments are anticipated
• a flexible instrument is realized, which can be rapidly adapted to changed circumstances.

Considering the fact that the European roll out of smart cards has not been completed in all application areas and not in all member states it is clear that debate on the smart card has not yet fully crystallized. This means that not all problems and solutions are known yet. Therefore as a short term activity the approach has been to set up cross--sectoral *Rules of Conduct*. These Rules of Conduct are general rules which still need to be worked out in more detail in a specific sectors. The health care sector for instance certainly needs detailed privacy rules in situations where there is a `health card ' with very sensitive personal data concerning medical care status and history. With these general codes of conduct, shape and content is given to the privacy principles mentioned above on the basic cross-sectoral level for smart cards.

These Rules of Conduct apply in addition to those already laid down in sectoral privacy codes of conduct.

The adoption of these Rules of Conduct demonstrate the responsible professionalism of the eESC constituents in this important user area of concern. It also demonstrates the need and wish to achieve a greater degree of standardization with regard to agreements and measures in the domain of privacy. At the same time, through these Rules of Conduct eESC service and application providers make clear to the consumer their co-responsibility for managing the data protection requirements of smart cards in personal privacy. They are confident that this will increase the willingness of the consumer to accept smart cards.

General model for a Privacy Code of conduct for interoperable smart card systems

The eESC smart card constituency,

Taking into consideration:

- that the eESC initiative aims to accelerate and harmonise the development of smart cards across Europe and to establish them in all shapes and forms as the preferred intelligent mobile and secure access key to citizen and business information society services;
- that the smart card has many different applications and can be applied in many sectors in an interoperable way;
- that in these applications the interests of all parties involved must always be considered and sometimes weighed against one another;
- that due to the many different applications and equipment used, the data collection, recording and use can become non-transparent to the card holder;
- that on the other hand the smart card offers possibilities to guarantee the safety of the data that are stored and to make the data that are stored more transparent by a direct form of consultation;
- that the privacy protection concerning the use of the smart card would benefit from openness with regard to all aspects of the information operation process;
- that this openness can also lead to stimulation of the social acceptance of the smart card;
- that, furthermore, attention should be paid to principles on a legal basis for collection and use limitation, purpose specification, data quality, card holder rights, security and the existing legal frameworks;
- that finally the safety and reliability of the smart card should be guaranteed,

also in view of:

- the European Directive 95/46/EC on the Protection of individuals with regard to the processing of personal data and the free movement of such data;
- the European Directive 97/66/EC concerning the processing of personal data and the protection of privacy in the telecommunication sector;
- National legislation in the Member States based on these Directives;

without prejudice to:

- the provisions of the national legislations and other formal and substantive legislation concerning data use and disclosure from the point of view of the smart card- related databases;
- (international) consumer conditions which have been set up in consultation with representative organizations;

and in so far as not yet provided for in sectoral privacy codes of conduct drawn up by representative organizations;

subscribes to the following Rules of Conduct for the protection of the interests of the consumer, which includes his personal data with regard to the use of smart cards in both the public and the private sector:

PARAGRAPH I: GENERAL PROVISIONS

Article 1: Definitions

In these Rules of onduct the following definitions are intended:

- *smart card*: a plastic card of a specific size and equipped with an electronic circuit consisting of one or more chips which can communicate with the outside world;
- *card holder*: a person who can be regarded as the rightful user of a smart card;
- *application*: a service which can be purchased by a card holder and/or his card proxy using a smart card;
- *personal card*: a smart card which is registered to a specific person or to whom the card can otherwise be traced;
- *card proxy*: a person who has been authorized by the card holder to make use of the smart card issued to the card holder, according to the rules of the application provider;
- *card issuer*: the party that issues the card to the card holder or has it issued, and that is responsible for the card management activities during the entire life cycle of the card;
- *card provider*: the party that on behalf of the card issuer issues the card to the card holder or has issued it;
- *smart card manufacturer*: the party that provides the smart chip to the card issuer and therewith reserves powers and responsibilities with regard to ordering and sound functioning of the chip, as well as concerning the allocation and separation of applications in the chip;
- *application provider*: the party offering an application system in which a smart card is used and who takes final responsibility of the proper functioning of the application;
- *service provider*: the party delivering a specific content or service to the card holder;
- *general card data*: a limited group of electronic data which can be used by application providers and, if applicable, by service providers;
- *personal data*: any information relating to an identified or identifiable natural person ('data subject');
- *processing of personal data*: any operation or set of operations which is performed upon personal data, whether or not by automatic means;
- *controller*: the party that alone or jointly with others determines the purposes and means of the processing of personal data;
- *processor*: the party that processes personal data on behalf of the controller;
- *third party*: any other party than the data subject, the controller, the processor and the persons who, under the direct authority of the controller or the processor, are authorized to process the data;
- *recipient*: the party to whom data are disclosed, whether a third party or not.

Article 2: Scope

These Rules of Conduct apply to smart cards containing personal data.

PARAGRAPH II: GENERAL CARD INTEGRITY ASPECTS

Article 3: Security

1. The card issuer is obliged to make such technical arrangements that application providers can take adequate security measures against abuse of the application and invasion of the card holder's personal environment.
2. The card issuer and the application providers are each responsible for the necessary technical and organizational facilities for protection of the personal data which have been put on the card under their responsibility, against accidental or unlawful destruction or accidental loss, alteration or unauthorized disclosure or access. The service provider is responsible for the correct execution of the security measures outlined by the card issuer and the application provider.

Article 4: Withdrawal of the card or of an application

1. The card holder is informed of the withdrawal by the card issuer, when the card itself is concerned, and by the application provider when a certain application is concerned.
2. Prior to the issuing of a smart card or the installation of a new application, measures are taken and procedures are developed with regard to neutralizing, erasing or destroying the data still present on the card in the case of withdrawal of the card or an application. Such a procedure may entail that the card holder is obliged to hand in or submit his smart card.

Article 5: Obligations of the card issuer

The card issuer specifies:

a. what applications may be installed on the card;
b. who may act as an application provider and as service providers and what responsibilities they have, all this according to statement of the application provider;
c. who can become card holders and under what conditions.

Article 6: Responsibilities of the card issuer

The card issuer is responsible for the management of general card data, as well as for clear structuring and, should the occasion arise, for dividing the chip into separate compartments for specific data for each application.

Article 7: Information

Unless the information concerned is already provided to the card holder by the application provider on the basis of an agreement between the card issuer and the application provider, the card issuer, before issuing the card to the card holder, is obliged to inform the latter at least on the following:

a. the identity of the card issuer;
b. the card applications that will be used at the time of issuing;
c. what the purposes are of processing in connection with the various applications, which he should have been or should be informed of by the application providers and by service providers;
d. who, at the time of the issuing of the card, will act as application providers and as service providers with reference to which application on the card and what powers they have, all this according to the statement of the application provider in question;

e. whether the card and use of the card or an application is part of a compulsory scheme (e.g. company identification or access card) or voluntary scheme and what the consequences of this are;
f. the obligations the card holder takes upon him when accepting the card;
g. to whom the card holders should refer in order to make use of the rights they have been granted as referred to in articles 16 ,17 and 18;
h. the facilities as referred to in article 9 and the procedures as referred to in article 10;
i. the mutual agreements between card issuer and card provider issuer, if a card provider has taken over these responsibilities and powers from the card issuer.

Article 8: Information in case of changes

In case of a change of one or more of the subjects as referred to in article 7, the card issuer is obliged to ensure, or to arrange with the application provider that there are procedures which provide for the card holder to be informed of the change and that it is indicated what its consequences are for the card holder.

Article 9: Help Desk

The card issuer, without prejudice to the own responsibility of the application provider, is obliged to provide a facility to which the card holder can refer with general questions concerning the card, the services that can be accessed or purchased with the card, the card issuer, the application providers and the service providers. The application provider is responsible for its own Help Desk function.

Article 10: Loss or theft

The card issuer is responsible for clear procedures for replacement and, if and in as far as possible, blocking of the card in case of loss, theft or mislaying of the card. This also includes rules and procedures in case of decease of the card holder.

PARAGRAPH III: GENERAL PRIVACY PRINCIPLES

Article 11: Increasing transparency

The application provider and the service provider are obliged:
a. to inform the card holder for the application(s) for which they are responsible, in view of the application in question, what the purpose is of the processing of the personal data;
b. b. to indicate and, upon request, inform the card holder of the connection, if any, with the related processing of personal data and who is the controller of this;

c. to inform the card holder upon request of the arrangements that have been made to enable data subject's right of access and rectification of the personal data and the way in which a card holder can use his right to object.Article 12: Starting point of the recognizability

The application provider and the service provider are obliged, if necessary for each compartment separately, to inform the card holder upon his request of which personal data are derived from the card or from the related processing of personal data in the use of the card.

Article 13: Stimulating carefulness

The application provider and the content or service provider are, considering the personal data they manage, are obliged to:

a. only put personal data on the card when it has been obtained fairly and lawfully;
b. ensure that the personal data are accurate, not excessive and, when necessary, kept up to date;
c. not to keep the personal data on the card any longer than is necessary with regard to the purpose of processing, in view of the application in question and without prejudice to the provisions of article 4 and the carefulness which should be observed with respect to the card holder;
d. to determine, and to inform the card holder of these aspects upon request, in which cases they are authorized to have access to the personal data in the related register of personal data;
e. to determine and at his request to inform the card holder, to which type of personal data they have access and which personal data they may store, change or erase.

Article 14: Principle of use limitation

The application provider and the service provider are obliged:

a. to describe the purpose of processing on the card in detail, to specify the processing clearly and to inform the card holder of it on his request;
b. to determine and to inform the card holder hereof upon request, for which purposes, in the light of the objective of processing, taking into account the application concerned, the personal data on the card will be used;
c. to use the personal data only for purposes which are compatible with the purpose for which the data are collected, in view of the card application in question;
d. only to put personal data on the card that are compatible with the goal of processing.

Article 15: Card issuer and general card data

The provisions as laid down in articles 11 through 14 apply equally to the card issuer with regard to the general card data.

PARAGRAPH IV: RIGHTS OF CARD HOLDERS

Article 16: Right of access to personal data

The card holder has, notwithstanding certain exceptions provided by law, the right of access to the personal data on the card concerning himself and the right to be informed about the source.

Article 17: Right of rectification, erasure or blocking

1. The card holder can request a card issuer, an application provider or service provider in writing to rectify, complete or erase the personal data concerning himself which have been put on the card, if these appear to be incorrect, incomplete or irrelevant for the purpose of the application, or contrary to statutory regulations.
2. The party addressed notifies within four weeks if, or to what degree, he complies with this request.

Article 18: Right to object

1. The card holder has the right to object at any time on compelling legitimate grounds relating to his particular situation to the processing of data relating to him. Where there is a justified objection, the processing may no longer involve these data.
2. The card holder has the right to object, on request and free of charge, to the processing of personal data relating to him which the controller anticipates being processed for the purpose of direct marketing.

PARAGRAPH V: FINAL PROVISIONS

Article 19: Smart card issuer

If issuance of the smart card is done by another organization (for example smart card manufacturer, processor or card provider under contract to the card issuer) which takes over certain responsibilities and powers from the card issuer, the card issuer nonetheless remains responsible for a clear delineation of the division of responsibilities and powers. The Rules of Conduct are then applied to card issuer and the card providing organization in accordance with this division.

Article 20: Complaint handling and appeal procedures

In so far as sectoral arrangements are not provided for, complaint handling and appeal procedures are developed with independent institutions to which card issuers, application providers and service providers conform.

Article 21: Publication of Rules of Conduct

These Rules of Conduct are part of the eESC Common Specifications Version 2. They are public and available without charge.

EXPLANATION FOR EACH ARTICLE

Rules of Conduct, which have been established on the basis of self-regulation, offer the possibility of laying down additional rules in certain fields. In this context, additional means that existing legislation and regulations (including existing sectoral privacy Rules of Conduct) continue in force and remain unimpaired. The related processing of personal data apply to the European Directives 95/46/EC and 97/66/EC and the national legislation in the Member States based on it. Controllers are for example obliged to notify the national supervisory authority. As the smart must be seen as a part of the information operating process to serve several related purposes, it is this process that must be notified. For that reason in the Rules of Conduct no attention is paid to the separate notification of a smart card. The other obligations based on the national legislation also continue in force and remain unimpaired. The additions based on the Rules of Conduct therefore mainly apply to the smart card itself. This means that the Rules of Conduct are only aimed at aspects which are specific for the use of the smart card as a part of the total information operation process.

Article 1

Taking into account this fact, only the concepts have been defined which are of importance for the smart card.
With regard to the actors and parts, next to the card holder (the person in who's name the card is and who generally uses the card) and the card proxy, it is especially the card issuer who is important. This is the party (see also article 6) which carries responsibility for the card and the organizational issues concerned with it. If a PKI infrastructure is included and (Certification Authority (CA) and Registration Authority (RA) services are at stake, it is the Card Issuer that still holds the overall responsibility not withstanding the responsibility of the CA and the liabilities this CA has on the basis of it's QCP (Qualified Certificate Policy).
In many cases it will also be the Card Issuer that installs the public identity (see Common Specifications: Citizen Certificate Guidelines) of the cardholder on the card. In this case the Card issuer holds all the responsibilities in relation to the process and content of the functionalities of identification, authentication and digital signature for non-repudiation.
Two other important actors are: the application provider and the service provider. The application provider is the party that provides a card application system, which means a coherent set of principles, rules and arrangements with regard to an application, including the card reading terminals belonging to the system. Examples of sector specific applications provided by means of the card concern for instance a public transport service, an eGovernment service, a health service or a payment service. This party also carries final responsibility for both the application and the data that are collected, stored and used with the help of this application. The service provider, not being the application provider, is the party which accepts the card and is therefore authorized to take cognizance of (part of) the data on the card (and sometimes of the related processing of personal data).
It is noted here that in the GIF model the Identification data are freely accessible; authentication data and digital signature data are protected by PIN and /or biometrics. Application provicers and service providers may read and use (by consent of the cardholder) the IAS data but are not allowed to change the content of these data. This is the sole responsibility of the Card Issuer.
The service provider may alter and use other data in conformity with the procedures of a card application. The service provider is not responsible for the card or for the applications loaded on it. However, he is responsible for his part of the activities, which he carries out in the total

information operation process around smart card services. Service providers may for instance be an information service on the internet that accepts the identification credentials of the cardholder.
From the point of view of privacy the most important actors, obviously apart from the card holder and card issuer, are the application provider and the service provider. After all, they are the ones who collect, process and use personal data of the card holder. However, it should be noted that these separated roles often overlap in practice, because they are often carried out by one actor. It will often occur that the card issuer is also the application provider. In the multi application environment this is obviously not the case.
General card data include both the card holder's personal data (in some cases being the GIF IAS data) and data concerning the card itself, such as serial and product numbers. The general data have been recorded electronically.

The definition of processing of personal data has been adopted from the European Directive 95/46/EC. The second part of the definition, in which all components of `any operation or set of operations' are specified, has been left out in the definitions.

Article 2

The Rules of Conduct are limited to personal cards, that is to say only to cards which can be traced to the person, regardless of whether they are used for a certain application by the card holder himself or by a card proxy. Impersonal cards (such as prepaid anonymous phone cards, pre paid anonymous parking cards, pre paid anonymous public transport cards etc.) do not fall within the scope of these Rules of Conduct. Articles 11 through 18 of the Rules of Conduct therefore only apply for the processing of personal data, meaning information relating to an identified of identifiable natural person. These articles have no significance for other data.

Article 3

The security of personal data is an issue of major importance. This applies both to the card and to the (reading) equipment which is used.
All aspects of a smart card system, including the smart card, the card readers, the network and the registration, must be protected adequately against unlawful access and illegal use. This means that the card issuer, application provider and service provider should take appropriate technical and organizational measures. These measures should ensure an appropriate level of security, taking into account the state of the art and the costs of their implementation in relation to the risks inherent in the processing and the nature of the data to be protected.
The most important role is that of the card issuer, who is to ensure that the basic technical facilities are present, so that the other parties involved can also take their own appropriate security measures. These includes compartmentalization of the card in such a way that, by means of technical facilities, unauthorized persons or organisations are prevented from taking cognizance of the personal data in a certain compartment and that data from the different compartments cannot be merged or matched. If there is a technical possibility that, using card readers, more data would become available to the application provider than necessary for the application, explicit agreements should be made with the application provider on data use and accompanying measures. The application provider is responsible for carrying out these measures properly.
After acceptance of the card, the card holder is obliged to treat it carefully and to observe the security measures indicated and other agreements. These agreements include preventing unlawful use of the card.

Article 4

Card holders should be informed of the fact that the card or an application is withdrawn. This must be done by the card issuer, when the entire card is withdrawn, and by the application provider when his application is withdrawn. When the card or part of it are not used any more, the data which were in use for processing should, preferably, be taken off the card as soon as possible. In practice this will not happen until the card holder offers the card to the application provider or a service provider. For these reasons the Rules of Conduct speak of neutralizing: the data cannot be used any more until that moment. Neutralizing can also take place by blocking the application or part of it from a central point. The erasure and destruction only applies in so far as this can be realized in practice.

Articles 5 and 6

The Rules of Conduct referring to the card issuer have been split up into powers and responsibilities. The powers are determining the applications and indicating in consultation with application providers which actors are involved in the card (application provider, service provider and card holder). The responsibilities are broader and in the first place include the technical aspects of the card. The card issuer must ensure that the card works properly. In addition, he is responsible for the management of the card, if necessary for dividing the card into different compartments and for the facility by means of which the application provider can put his application on the card. In effect, the Rules of Conduct specify scaled responsibility. The card issuer is responsible for the card, the technical facilities and the general data, the application provider for that concrete application and the application data. This division of roles is in line with current practice. Should these role patterns change in the course of time, this will be taken into account when adjusting these rules (see article 19).

Article 7

As has been worded clearly in the preamble, openness with regard to all aspects of smart card use is of utmost importance. This way confidence in the card can be increased, unjust feelings of privacy invasion can be decreased and partly through this, the willingness for acceptance by the consumer can be promoted. It is therefore important to inform the card holder, before the card is issued, of its applications, whether it concerns a closed user group in which participation is obliged or an open user group, in which participation takes place voluntarily. An example of a closed user group is the company pass which employees must have on them. An open user group is for instance a customer card. The card holder should also be informed of the obligations he takes upon himself when accepting the card and he receives a list of all (groups of) application providers. Of special importance with regard to the openness about the card is the insight into the data concerning the card holder, which are collected with use and are stored either on the card or in the related register of personal data and what data will be displayed when the card holder offers his card to the infrastructure of a service provider either in an on-line or off-line situation

Article 8

In view of the preceding, it is obvious that the card holder will be informed of changes in one or more of the aspects mentioned above. The card holder can then determine his course of action, depending on the consequences.

Articles 9 and 10

With regard to the smart card (this also applies unimpaired for other types of card), the dangers of theft or loss of the card are pointed out repeatedly. For a card with more than one application it is important that the card holder is not sent from pillar to post in this case. A central institution where the card can be blocked and where a completely reconstructed card can be applied for, is desirable. With regard to privacy, it must not be possible to reconstruct all data on the card in one central place in the case of a card with more than one application. A central institution can, however, be useful in approaching individual application providers for the reconstruction of their part of the card. In the case of a GIF smart card community this central role may be fulfilled by the Smart card community administrator.

Article 11

In addition to the openness which the card issuer should observe, there are separate responsibilities for the application provider and the service provider. In their case this mainly concerns openness with regard to their processing of personal data of the card holder. Depending on the concrete application, various data closely related to the application, can be recorded on the card, . It is therefore important that they inform the card holders of the objective of processing, their relationship to the related registers and the arrangements that have been made to enable the realization of the rights to access and rectification that are granted in the European Directive and implemented in national legislation. Furthermore, there is the obligation to indicate who is the controller of the related processing of personal data, if this is not the application provider or the service provider himself. This information is especially important if the card holder wishes to exercise his rights in reference to the related processing of personal data.

Article 12

The smart card can also be used to collect data on the service provider. It may , for instance, be possible to determine where a person was at a certain time or what products were purchased. The application provider and the service provider should inform the card holder at his request of which data are recorded in a certain situation.

Article 13

Material standards by which controllers of processing of personal data undertake to carefully treat the personal data of the data subjects are an essential part of the European Directive. This article lists these material norms for the card. In addition, there is the obligation to determine what data are accessible to an application provider and a service provider and under whose responsibility data have been captured, changed or erased. This information should be disclosed to the card holder upon request. Transparency is also needed in relation to the data in the related processing.

Article 14

The principle of use limitation is often identified as the most important. After all, invasion of privacy is often identified with the use of data for entirely different purposes than stated at time of capture. In the case of the multi-application smart card, the use limitation principle can be implemented in a technical sense by dividing cards into different compartments. The use limitation principle applies for each of these compartments. Part of this is the agreement that the application provider or service provider may only take cognizance of or make use of data in the compartment assigned to him, unless the card holder has given his explicit consent

for broader cognizance or use. This practical implementation of use limitation principle helps remove the fear that all data on a card can be used or exchanged by anyone.
It determines that the purpose of processing should be described as accurately as possible and that data may not be used for purposes which are incompatible with that objective. This goal of processing is determined by the application. Another aspect of the use limitation principle is that no more data may be recorded on the card than are in keeping with the objective of processing.

Article 15

This article expresses that the privacy principles also apply to the card issuer in so far as it concerns general card data, which are managed by him.

Articles 16, 17 and 18

The rights of the data subjects mostly correspond to the rights as described in the European Directive. However, those rights only apply to the data subject himself. This is generally the card holder. Caution should be observed with regard to data which are traceable to other persons, if any. It does not go without saying that the transaction data of the card proxy can be consulted. With respect to minors who have not yet reached the age of sixteen, the requests can be made by statutory representatives.
For instance, with regard to the right to access, the same exceptions apply as referred to in the European Directive, the most important of which is that access may be declined when this is necessary in view of the protection of the data subject and of the rights and freedoms of others, including the processor.
Also with regard to the right to rectification, erasure or completion, the provisions of the Directive fully apply. Rectification, erasure or completion of data on the card can have consequences for related registers and vice versa.
A relative new right is the right to object when data are used or are intended to be used for the purpose of direct marketing. This right to object is absolute in the sense that the processing in that case may no longer involve those data. Next to this absolute right there is a relative right for the data subject to object on compelling legitimate grounds relating to his particular situation. In that case the controller is obliged to weigh up his interest in processing the data of this particular data subject against the interests of that data subject. Where there is a justified objection the controller may not longer process the data.

Article 19

Practice shows that more and more often the card issuer is not in complete command of purchase, organization and management of the chip. EMV and CEPS compliant cards are clear examples of this (card compliant with debit/credit card specifications and with ePurse specifications are examples of this.) This applies to cases in which the card issuer obtains the chip from a party (called card provider) which reserves several rights. In such cases, there should be a clear picture of the division of responsibilities and powers between card issuer and card provider.

Articles 20 through 21

Rules of conduct are only complete when an independent complaints handling and appeal procedure is provided for. These procedures leave the possibility open for the card holder to appeal to the national supervisory authority of the relevant Member State.