Open Smart Card Infrastructure for Europe

v2

Volume 4: **Public Electronic Identity, Electronic Signature and PKI**

Part 2: **Study on legal issues in relation to the use of public Electronic Identity**

Authors: **Expert Report for eESC TB1 Public Identity**

Study on legal issues in relation to the use of public Electronic Identity

Overview of the Study

The objective of this mission is to prepare a study on legal issues in relation to the use of public Electronic Identity, taking into account the relevant European regulations, such as:

- EU Directive on the protection of individuals with regard to the processing of personal data and on the free movement of such data (95/46/EC)
- Data Protection Regulation (01/45/EC) as well as
- 2001/497/46/EC Commission Decision on standard contractual clauses for the transfer of personal data to third countries under Directive 95/66/EC

and taking into account the

- DIRECTIVE 1999/93/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 13 December 1999 on a Community framework for electronic signatures.

The study should identify and describe briefly the juridical issues that are at stake and make some recommendations. The study should also cover the specific issues raised by the transfer of personal (EID) data trans-border.

The study will take into account an existing report prepared by Holvast & Partners on a "privacy code of conduct" in smart card and e-service applications handling data affected by European data protection regulations.

Stefan Engel-Flechsig
Radicchio Ltd. UK
15th October 2002

Table of Contents

Overview 2
1. The EID concept 5
2. Data protection regulations in the EU and relevance for the EID concept 9
2.1. Introduction 9
2.1.1. Directive 95/46 EC on the Protection of individuals with regard to the processing of personal data and on the free movement of such data 9
2.1.2. Decision of the European Commission 2001/497 EC 10
2.1.3. Directive 97/66 EC on processing of personal data and the protection of privacy in the telecommunications sector 11
2.1.4. Directive 01/45 EC on the processing of personal data by the Community institutions and bodies and on the free movement of such data 12
2.1.5. Directive 99/93 EC on a Community Framework for Electronic Signatures 13
2.1.6. Directive 2000/31 EC on a Legal Framework for Electronic Commerce 14
2.1.7. Relevance of Directives and Decisions to the EID concept 16
3. Data protection and the EID concept 17
3.1. Directive 95/46 EC and the EID concept 17
3.1.1. Scope of the Directive 95/46 EC 17
3.1.1.1. General scope and applicable law, Article 3 and Article 4 17
3.1.1.2. EID concept 18
3.1.2. Definitions 19
3.1.2.1. Key definitions of the Directive 20
3.1.2.2. EID concept 20
3.1.3. General rules for lawful processing of personal data 23
3.1.3.1. General rules of the Directive 23
3.1.3.1.1. Data quality, Article 6 23
3.1.3.1.2. Criteria for legitimate data processing, Article 7 and Article 8 23
3.1.3.2. EID concept 25
3.1.3.2.1. EID concept and data quality 25
3.1.3.2.2. EID concept and criteria for legitimate data processing 26
3.1.4. Confidentiality and security of processing of personal data 27
3.1.4.1. Confidentiality and security, Article 16 and Article 17 27
3.1.4.2. EID concept 28
3.1.4.2.1. Confidentiality 28
3.1.4.2.2. Technical security 28
3.1.5. Data subject's rights 29
3.1.5.1. Data subject's rights, Articles 10, 11, 12, 13, 14 30
3.1.5.2. EID concept 30
3.1.5.2.1. Information to the data subject, Article 10 and Article 11 30
3.1.5.2.2. Rights to access, rectification, erasure and blocking, Article 12 32
3.1.5.2.3. Right to object, Article 14 32
3.1.6. Notification, Articles 18 and 19 32
3.1.7. Codes of conduct 33
3.1.7.1. Codes of conduct, Article 27 33
3.1.7.2. EID concept 33
3.1.8. Transfer of personal data to third countries 36

3.1.8.1. Transfer of personal data to third countries, Article 25 and Article 26 36
3.1.8.2. EID concept 37
3.2. Decision on model clauses 01/497 EC and the EID concept 38
3.3. Directive 99/93 EC on electronic signatures and data protection 40
3.3.1. Data protection provision 40
3.3.4. EID concept 40
3.4. Directive on e-commerce 00/31 EC 41
3.4.1. Directive on e-commerce and data protection 41
3.4.2. EID concept 41
4. Summary Conclusions for EID 43
4.1. General conclusions 43
4.2. Conclusions as regards data protection and EID 44
4.3. Conclusions as regards next steps 46
Annex 1: Overview on national data protection legislation, February 2002 48
Annex 2: Overview on EU directives and decisions on data protection and privacy 51

1. The EID concept

The primary objective of Trailblazer 1 within the eEurope SmartCard Charta activity is to establish minimum requirements for a common public identity token which can be used for services like electronic signatures, authentication and, possibly, encryption.

The benefits of the establishment of such minimum requirements will be:

- an important step towards e-government in the European member states,
- increased trust and confidence via enhanced data security,
- promotion of European commerce and online payments.

The goals are:

- Minimum requirements for electronic public identity tokens. On the basis of these requirements participating member states can recognize the public identity token issued in other member states.
- Member states will be able to read and verify a public identity token. The goal is to bring out recommendations on how this should be done.

The public identity token is not so much a replacement of the physical document as an addition. It is a token for an electronic environment as opposed to the traditional document for the physical environment.

The Public Identity Token is defined as an identity token accepted by public authorities in the country where it is issued. The compliant token should be accepted in all countries that issue similar tokens.

Electronic Identity Card (EID-card):

A smart card based token, containing private keys and corresponding public key certificates. Optionally, the card may also contain a visual identity document.

The EID-card can be used by a citizen

- for electronic identification and authentication to public and private on-line services
- for qualified electronic signatures conforming to the EU directive
- optionally for confidentiality services, enabling encryption of data transmitted over a network
- optionally as an official travel document within the EU. However, this requires that the smart card based Public Identity token also contains a visual identity document.

The EID-card could be used for many different fields of application, like

- health insurance,
- social security,
- public transport, or
- financial transactions.

Additional data or applications can be stored in the on-board memory of the card. These data or applications can support international interoperability like travel documents or be country-specific or they can be chosen by the card holder (citizen).

Figure 1 gives an overall perspective on possible relationships between the possible legal entities involved in the process of an EID.

These legal entities or organisational units are in principle:

1. The issuer of EID-card, usually the government as identity service provider,
2. The holder of EID-card, usually the citizen,
3. The public sector offering services or applications by using the EID-card,
4. The private sector offering services or applications by using the EID-card,
5. The certification service provider providing the necessary infrastructure and processes for issuing certificates, managing certificate requests and revocation of certificates on the EID-card.

Between these organisational units manifold information relationships are possible, e.g.

1. the citizen asks for the issuance of an EID with his/her governmental identity service provider;
2. the citizen using his/her EID to ask for a specific public service from a specific public agency in his/her home-country,
3. the public agency in one specific country may ask another agency or a private organisation to provide a specific service,
4. a private company provides services to the citizen.

The information relationships may be in one specific country, thus following the national regulations only, and/or the relationship might be a trans-border service or application, thus asking for a multi-country legal assessment.

The EID aims to build a universally recognized electronic ID token for identifying citizens in multiple use case scenarios. The EID will make it possible to pass the identity, once issued from one legal entity into other existing infrastructures of applications, whether in the public or private sector. In addition the EID will use certification service providers, most probably in the different national legislations. This proposal takes into account different functionalities and builds on various processes. From that perspective it is justified to speak not of the EID but rather of the “EID concept”.

Taking these various use-cases into account the necessary functionality of the EID concept can be described as follows:

1. multipoint communication
2. openness and transparency
3. universal recognition and interoperability.

Two main areas of interest have to be addressed from a legal and regulatory point of view:

1. What are the existing regulatory areas which are related to EID, and what are the legal requirements for the various parties and functions involved in EID processes in regard to data protection?
2. What are the regulatory possibilities to address the trans-border communication and the interoperability needed for the universal recognition of EID?

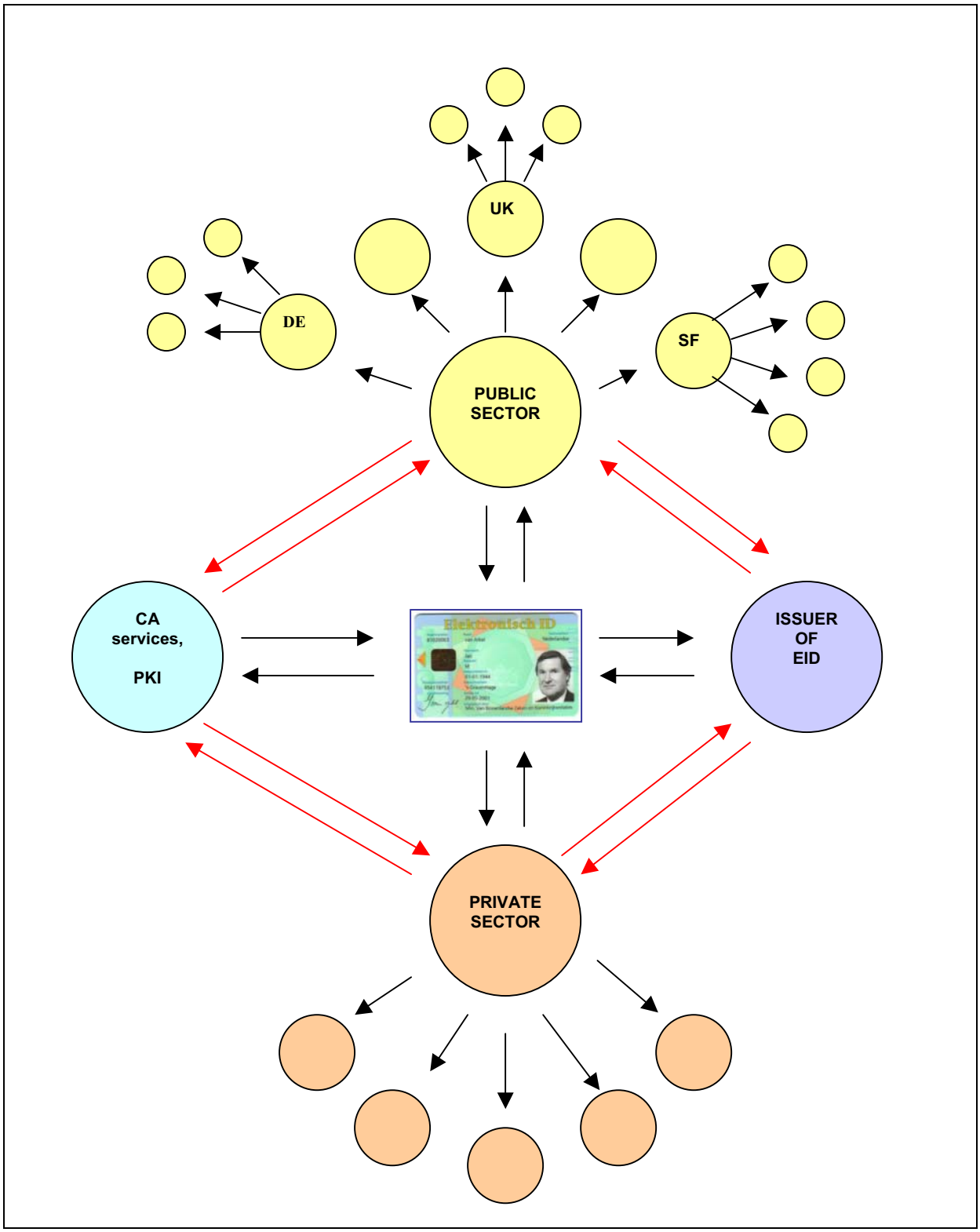

FIGURE 1: POSSIBLE RELATIONSHIPS BETWEEN LEGAL ENTITIES

The study has to be seen in the context of the eESC activities. eESC has identified the issues and an outline action plan for their resolution in order that smart cards can help to fulfil the expectations of citizens within the information society. At the end of 2000, eESC published the Common Requirements[1], a document containing the action plans and deliverables of the 12 eESC Trailblazer working groups. The action plan addresses both the citizens' needs and those of the business community in terms of business cases, multi-functionality and interoperability of systems and infrastructure, as well as the provision of trust in all aspects of service delivery. The overall outcome of these action plans is being consolidated in a set of eESC Specifications to be concluded at the end of 2002 and launched early in 2003.

As a part of these common specifications, a Global Interoperability Framework (GIF) for Identification, Authentication and Electronic Signature (IAS) has been developed. Its aim is to facilitate interoperability between the various IAS schemes emerging in Europe and more widely throughout the world.

The vision driving GIF is the high expectation of smart cards as "The intelligent key to *e*-services" for all citizens in the domains of local and trans-national Government. This perspective will be taken by the legal study.

It has to be noted that, in most cases, the roles of the different sectors are clearly defined in their specific areas of national regulations and thus the legal requirements follow the specific national legislation and the existing national legal organisational framework; e.g. the various European Member States have national data protection legislation and a matching national organisation. Although the European Directive 95/46 EC aims for harmonisation in European data protection, the differences in the various national data protection laws might be significant, e.g. the use of codes of conducts are accepted in some Member States, but not in others. This leads to a more complex legal assessment.

Moreover, the legal assessment becomes more complex if, in addition to the various national areas of regulation, other geographical areas like e.g. the US or Japan have to be included in the EID concept. The European Union clearly has the most regulated environment as regards data protection and electronic signatures. US regulation tends to be more pragmatic than EU regulation and hence more flexible. Other regions of the world do not reach the level of US/European regulations.

In a universal EID concept it is crucial to identify what regulation has to be taken into account and what legislation the infrastructure will refer to. As the EID concept is in the first place a European activity which will be available in the European Union, the legal study has to start with the European regulations on data protection and electronic signatures; in a second step the legal implications outside the European Union have to be taken into account.

This overview on legal implications will provide an overview on the regulatory areas related to EID and data protection (**chapter 2**), the main regulatory areas related to EID and data protection (**chapter 3**) and will summarize conclusions for issues to be addressed in the next steps (**chapter 4**).

The overview will concentrate on the **European regulations**.

[1] See the document "eEurope Smart Cards Common Requirements: Executive summary" available on the website of eESC; see also the GIF documents on IAS Part 1 and Part 2 available as OSCIE v2 Vol 3 parts 1 and 2;

The overview refers to the **"Rules of Conduct for privacy and card integrity"**[2], version 01.1, where appropriate, prepared by Holvast & Partner.

2. Data protection regulations in the EU and relevance for the EID concept

2.1. Introduction

The European Union has an advanced regulatory framework for the protection of personal data:

- The European Directive relating directly to data protection is the Directive 95/46 EC of the European Parliament and the Council of 24th October 1995 on the Protection of individuals with regard to the processing of personal data and on the free movement of such data.[3]
- The European Commission has adopted a Decision 01/497 EC setting out standard contractual clauses ensuring adequate safeguards for personal data transferred from the EU to countries outside the Union.[4]
- Directive 97/66 EC of the European Parliament and of the Council of 15th December 1997 concerning the processing of personal data and the protection of privacy in the telecommunications sector.[5]
- The European Parliament and the Council of Ministers have adopted the Regulation on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data, Directive 01/45 EC.[6]
- The European Parliament and the Council of Ministers have adopted the Directive 99/93 EC of 13th December 1999 on a Community Framework for Electronic Signatures.[7]
- The European Parliament and the Council of Ministers have adopted the Directive on a Legal Framework for Electronic Commerce 00/31 EC, which was adopted on 8th June 2000.[8]

Some directives relate directly to the protection of personal data, i.e. the Directive 95/46 EC, the Directive 97/66 EC, the Directive 01/45 EC and the decision 01/497 EC, whereas the other Directives refer to the regulation of different topics but refer to the data protection directives, especially to the Directive 95/46 EC.

2.1.1. Directive 95/46 EC on the Protection of individuals with regard to the processing of personal data and on the free movement of such data

The objects of the Directive 95/46 EC are to protect the fundamental rights and freedoms of natural persons, and in particular their right to privacy with respect to the processing of personal data and to prevent any restriction or prohibition on the free flow of personal data between Member States for reasons connected with the protection of personal data.

The Directive 95/46 EC lays down common rules, to be observed by those who collect, hold or transmit personal data as part of their economic or administrative activities or in the course

[2] Referred to as "Code of Conduct"

[3] Official Journal L 281, 23/11/1995 P. 0031 - 0050

[4] Official Journal L 181, 4/7/2001 P. 0019 - 0031

[5] Official Journal L L 024 , 30/01/1998 P. 0001 - 0008

[6] Official Journal L 008, 12/01/2001, P. 0001 - 0022

[7] Official Journal L 13, 19.1.2000, P. 0012 - 0020

[8] Official Journal L 178, 17/07/2000, P. 0001 - 0016

of the activities of their association. The Directive 95/46 EC sets out basic principles and rules for the collation and keeping of personal data about individuals, placing clear obligations upon those who wish to do so in respect of how that data may be collected and processed, for what purposes it may be used (i.e. those for which it was collected) and for data quality as well as for security and confidentiality of processing.

In order to remove the obstacles to the free movement of data while guaranteeing the protection of the right to privacy, the European Directive 95/46/EC aims at harmonising the national provisions in this field.

The Member States of the EU have been required to put their national legislation in line with the provisions of the directive by 24th October 1998. Most member countries have fulfilled these requirements by now. For a detailled list see **Annex 1.**

The Directive 95/46 EC contains 7 chapters which define the following regulations:

1. Chapter 1: General principles on

    a. the object of the Directive;
    b. the definitions of personal data, processing of personal data, personal filing systems, controller, processor, third party and recipient;
    c. the scope of the directive; and
    d. the national applicable law.

2. Chapter 2: General rules on the lawfulness of the processing of personal data, including:

    a. principles relating to data quality,
    b. criteria for making data processing legitimate;
    c. special categories for data processing;
    d. information to be given to the data subject;
    e. the data subject's right of access to data;
    f. exemptions and restrictions;
    g. the data subject's right to object;
    h. confidentiality and security of processing of personal data; and
    i. notification of the supervisory authorities.

3. Chapter 3: Judicial remedies, liability and sanctions;
4. Chapter 4: Transfer of personal data to third countries;
5. Chapter 5: Codes of conduct;
6. Chapter 6: Supervisory authorities;
7. Chapter 7: Communitiy implementing measures and final provisions.

The Directive is the basic reference document for all data protection provisions in specific areas.

2.1.2. Decision of the European Commission 2001/497 EC

In addition to the Directive 95/46 EC the European Commission has adopted a **Decision 2001/497 EC**[9] setting out standard contractual clauses ensuring adequate safeguards for personal data transferred from the EU to countries outside the Union. The Decision obliges Member States to recognise that companies or organisations using such standard clauses in

[9] Official Journal L 181, 4/7/2001 P. 19 - 31

contracts concerning personal data transfers to countries outside the EU are offering "adequate protection" to the data. Use of these standard contractual clauses will be voluntary but will offer companies and organisations a straightforward means of complying with their obligation to ensure "adequate protection" for personal data transferred to countries outside the EU which have not been recognised by the Commission as providing adequate protection for such data.

So far, only Switzerland, Hungary and the US 'Safe Harbor' arrangement have been recognised as providing adequate protection.

2.1.3. Directive 97/66 EC on processing of personal data and the protection of privacy in the telecommunications sector

This Directive applies to the processing of personal data in connection with the provision of publicly available telecommunications services in public telecommunications networks in the Community, in particular via the Integrated Services Digital Network (ISDN) and public digital mobile networks. Member States had to bring into force the laws, regulations and administrative provisions necessary for them to comply with this Directive not later than 24 October 1998. Most European member countries have implemented the Directive.

The provisions of the Directive are aimed at protecting, by supplementing the general data protection Directive 95/46/EC, the fundamental rights of natural persons and particularly their right to privacy, as well as the legitimate interests of legal persons in the area of telecommunications and mobile networks by introducing specific legal, regulatory, and technical provisions, in particular with regard to the increasing risk connected with automated storage and processing of data relating to subscribers and users.

The Directive takes into account the new advanced digital technologies introduced in public telecommunications networks, which gave rise to specific requirements concerning the protection of personal data and privacy of the user. More specifically the Directive takes into account the development of the information society, characterised by the introduction of new telecommunications services and the cross-border development of these services, such as video-on-demand, interactive television. The success of these services is from the Directive's standpoint partly dependent on the confidence of the users that their privacy will not be at risk.

Measures must be taken to prevent the unauthorised access to communications in order to protect the confidentiality of communications by means of public telecommunications networks and publicly available telecommunications services; whereas national legislation in some Member States only prohibits intentional unauthorized access to communications.

Data relating to subscribers processed to establish calls, containing information on the private life of natural persons and concerning the right to respect for their correspondence or concerning the legitimate interests of legal persons; may only be stored to the extent that is necessary for the provision of the service for the purpose of billing and for interconnection payments, and for a limited time. Any further processing which the provider of the publicly available telecommunications services may want to perform for the marketing of its own telecommunications services may only be allowed if the subscriber has agreed to this on the basis of accurate and full information given by the provider of the publicly available telecommunications services about the types of further processing he intends to perform.

The introduction of itemized bills has improved the possibilities for the subscriber to verify the correctness of the fees charged by the service provider; the Directive recognizes that, at the same time, it may jeopardise the privacy of the users of publicly available

telecommunications services and therefore Member States must encourage the development of telecommunications service options such as alternative payment facilities which allow anonymous or strictly private access to publicly available telecommunications services, for example calling cards and facilities for payment by credit card; alternatively, Member States may, for the same purpose, require the deletion of a certain number of digits from the called numbers mentioned in itemized bills.

As regards calling line identification, it is necessary to protect the right of the calling party to withhold the presentation of the identification of the line from which the call is being made and the right of the called party to reject calls from unidentified lines. It is justified to override the elimination of calling line identification presentation in specific cases; whereas certain subscribers, in particular help lines and similar organizations, have an interest in guaranteeing the anonymity of their callers.

As regards connected line identification, it is necessary to protect the right and the legitimate interest of the called party to withhold the presentation of the identification of the line to which the calling party is actually connected, in particular in the case of forwarded calls; the providers of publicly available telecommunications services must inform their subscribers of the existence of calling and connected line identification in the network and of all services which are offered on the basis of calling and connected line identification and about the privacy options which are available; this will allow the subscribers to make an informed choice about the privacy facilities they may want to use; the privacy options which are offered on a per-line basis do not necessarily have to be available as an automatic network service but may be obtainable through a simple request to the provider of the publicly available telecommunications service;.

Safeguards must be provided for subscribers against the nuisance which may be caused by automatic call forwarding by others; in such cases, it must be possible for subscribers to stop the forwarded calls being passed on to their terminals by simple request to the provider of the publicly available telecommunications service.

In case the rights of the users and subscribers are not respected, national legislation must provide for judicial remedy; whereas sanctions must be imposed on any person, whether governed by private or public law, who fails to comply with the national measures taken under this Directive.

2.1.4. Directive 01/45 EC on the processing of personal data by the Community institutions and bodies and on the free movement of such data

The aim of the Regulation is to protect individuals' freedom and fundamental rights, particularly in their private life. Article 3 specifically states that it applies to all Community institutions and bodies, insofar as the processing of personal data is carried out in the exercise of activities all or part of which fall within the scope of Community law.

The Regulation applies to the processing of data by the following institutions: the European Parliament, the Council of the Union, the European Commission, the Court of Justice and the Court of Auditors. The bodies set up by the EC, ECSC and EAEC Treaties are also included: the European Central Bank, the European Investment Bank, the Economic and Social Committee, the Committee of the Regions. Lastly, it also applies to bodies set up under secondary Community legislation, namely: the European Centre for the Development of Vocational Training, the European Foundation for the Improvement of Living and Working Conditions, the European Environment Agency, the European Training Foundation, the European Monitoring Centre for Drugs and Drug Addiction, the European Agency for the Evaluation of Medicinal Products, the Office for Harmonisation in the Internal Market (trade

marks and designs), the European Agency for Safety and Health at Work, the Community Plant Variety Office and the Translation Centre for the Bodies of the Union.

The institutions and bodies dealing with personal data are obliged to supply the relevant information to the person concerned, allowing them to exercise the rights provided for by the Regulation. The data subject also has the right to obtain access to these data and to have them rectified, blocked or erased under the conditions set out in the Regulation, as well as to object to the processing of these data under certain circumstances. The institutions and bodies may nevertheless derogate from some of these rights for clearly defined reasons in the public interest.

Moreover, the regulation establishes an independent control authority, the European Data Protection Supervisor. Specific guarantees have been put in place to ensure his or her independence, in particular as regards appointment and dismissal, term of office and the requirement that he or she should not seek or take instructions from anybody. The controller is responsible for ensuring that the provisions of the Regulation are implemented. In addition, each institution and body must designate at least one person as Data Protection Officer; this person who cooperates with the controller and is responsible for ensuring, in an independent manner, that the Regulation is applied within each institution and body.

2.1.5. Directive 99/93 EC on a Community Framework for Electronic Signatures

The European Union has introduced a legal framework to guarantee EU-wide recognition of electronic signatures – a prerequisite for ensuring the security of data that are transmitted electronically (Directive 1999/93/EC of the European Parliamnet and of the Council of 13 December 1999 on a Community Framework for Electronic Signatures).

The purpose of the Directive is to facilitate the use of electronic signatures and to contribute to their legal recognition. It establishes a framework for electronic signatures and certain certification services in order to ensure the proper functioning of the internal market.

The Electronic Signature Directive defines the requirements for electronic signatures, certificates and certification services, to ensure “minimum levels of security” and allow their free movement throughout the Union**.** European Member States had to implement their laws, regulations, and administrative provisions necessary to comply with this directive before July 19, 2001. After two years of implementation, the European Commission will carry out a review of the Directive to ensure, inter alia, that the advances in technology or changes of the legal environment have not created barriers to the aims of the Directive. The European Commission has to review the operation of the Directive and report to the European Parliament and to the European Council by 19th July 2003 at the latest.

The directive stipulates that, generally speaking, an electronic signature cannot be legally discriminated solely because it is in electronic form. For example, any kind of electronic signature can be admissible to courts and can be used as evidence in legal proceedings. If a certificate, the service provider, and the signature product used meet a set of clearly defined specific requirements, there will be an automatic assumption that any resulting electronic signatures (advanced electronic signatures) are just as legally valid as a hand-written signature. All products and services related to electronic signatures can circulate freely and are only subject to legislation and control by the country of origin. Member states cannot make the provision of services related to electronic signatures subject to mandatory licensing. The legislation establishes minimum liability rules for service providers who would, in particular, be liable for the validity of a certificate's content. This approach ensures the free movement of certificates and certification services within the internal market, builds consumer trust, and stimulates operators to develop secure systems and signatures without

restrictive and inflexible regulation. Given the pace of technological innovation, the legislation provides for legal recognition of electronic signatures irrespective of the technology used (e.g. digital signatures using asymmetric cryptography or biometrics).

The legislation covers certificates that are supplied to the public for identifying the sender of an electronic message. Nevertheless, in accordance with the principles of party autonomy and contractual freedom, it does permit the operation of systems governed by private law agreements such as corporate Intranets or banking systems, where a relation of trust already exists and there is no obvious need for regulation. By this, the Directive only wants to contribute to the use and legal recognition of electronic signatures within the European Community; a regulatory framework is not needed for electronic signatures used within systems, which are based on voluntary agreements under private law between a specified number of participants. The Directive wants to respect the freedom of parties to agree among themselves the terms and conditions under which they accept electronically signed data to the extent allowed by national law.

To promote a global market in electronic commerce, the legislation includes mechanisms for co-operation with third countries based on mutual recognition of certificates and on bilateral and multilateral agreements.

A certification authority (CA) that operates in accordance with Annex II (requirements for certification service providers issuing qualified certificates) of the Directive shall operate a certification authority service in accordance with these main obligations.

Detailed technical specification of the requirements for qualified certificates, certification service providers and secure signature creation devices that are generally provided for in the Annexes will have to be officially endorsed by the Article 9 Committee which has been tasked by the Directive to follow the technical developments. Suggestions related to these specifications have been discussed and agreed upon within the scope of the European Electronic Signature Standardization Initiative (EESSI). Proposals for Secure Signature Creation Devices, for a general format for Advanced Electronic Signatures, for Qualified Certificate Profiles, for Policies for Certification Providers issuing Qualified Certificates, for Time Stamping Profiles and for Procedures for Electronic Signature Verification have already been published and circulated for comment.

The European Directive on electronic signatures had to be implemented into national legislation by 19th July 2001. Most of the European Member countries have finished this process. This means that in any case of offering certificates the specific national legislation has to be taken into account and watched carefully.

2.1.6. Directive 2000/31 EC on a Legal Framework for Electronic Commerce

The Directive on a Legal Framework for Electronic Commerce Directive 2000/31/EC was adopted on 8th June 2000. Member States had 18 months in which to implement the Directive into national law following its publication in the EU's Official Journal. Most of the European member states had adopted the Directive's principles into the national regulatory framework by 17th January 2002.

The rationale for adopting the Directive was the unanimous opinion of the European member states that the global electronic commerce market is growing extremely fast and could be worth $ 1.4 trillion by the year 2003 (source: Forrester Research). In Europe, electronic commerce is already worth 17 billion euro and is expected to reach 340 billion euro by 2003.

The Directive covers **all Information Society services**, both business to business and business to consumer, and **services provided free of charge to the recipient** e.g. funded by advertising or sponsorship revenue and services allowing for on-line electronic transactions such as interactive tele-shopping of goods and services and on-line shopping malls. Examples of sectors and activities covered include on-line newspapers, on-line databases, on-line financial services, on-line professional services (such as lawyers, doctors, accountants, estate agents), on-line entertainment services such as video on demand, on-line direct marketing and advertising and services providing access to the World Wide Web.

The Directive applies **only to service providers established within the EU** and not those established outside. However, the Directive takes particular care to avoid incompatibility and inconsistency with legal developments in other parts of the world so as to avoid obstacles to global electronic commerce. Moreover, in some areas the Directive provides for solutions that may serve as a model at international level, thus reinforcing Europe's influence on the development of an international legal framework.

The Directive defines the **place of establishment** as the place where an operator actually pursues an economic activity through a fixed establishment, irrespective of where web-sites or servers are situated or where the operator may have a mail box. This definition is in line with the principles established by the EC Treaty and the case law of the European Court of Justice. Such a definition will remove current legal uncertainty and ensure that operators cannot evade supervision, as they will be subject to supervision in the Member State where they are established. The Directive prohibits Member States from imposing special authorisation schemes for Information Society services which are not applied to the same services provided by other means. It also requires Member States to oblige Information Society service providers to make available to customers and competent authorities in an easily accessible and permanent form basic information concerning their activities (name, address, e-mail address, trade register number, professional authorisation and membership of professional bodies where applicable, VAT number).

The proposal obliges Member States to remove any prohibitions or restrictions on the use of electronic contracts. In addition, the proposal will ensure legal security by imposing certain information requirements for the conclusion of electronic contracts in particular in order to help consumers to avoid technical errors. These provisions will **complement the Directive on Electronic Signatures**.

To eliminate existing legal uncertainties and to avoid divergent approaches between Member States, the Directive establishes an **exemption from liability for intermediaries** where they play a passive role as a "mere conduit" of information from third parties and limits service providers' liability for other "intermediary" activities such as the storage of information. The Directive strikes a careful balance between the different interests involved in order to stimulate co-operation between different parties and so reduce the risk of illegal activity on-line.

The Directive defines **commercial communications** (such as advertising and direct marketing) and makes them subject to certain transparency requirements to ensure consumer confidence and fair trading. So that consumers may react more readily to harmful intrusion, the Directive requires that commercial communications by e-mail are clearly identifiable. In addition, for regulated professions (such as lawyers or accountants), the Directive lays down the general principle that the on-line provision of services is permitted and that national rules on advertising shall not prevent professions from operating Web-sites. However, this will have to respect certain rules of professional ethics, which should be reflected in codes of conduct to be drawn up by professional associations. From a mobile commerce point of view – at least as long as the information on a mobile device is restricted

– this will have some effect on mobile commerce and could make the fulfilment of this transparency practically impossible.

The Directive seeks to strengthen mechanisms to ensure that existing EU and national legislation is enforced. This includes encouraging the development of **codes of conduct at EU level,** stimulating administrative co-operation between Member States and facilitating the setting up of effective, alternative cross-border on-line dispute settlement systems. The Directive also requires Member States to provide for fast, efficient legal redress appropriate to the on-line environment and to ensure that sanctions for violations of the rules established under the Directive are effective, proportionate and dissuasive.

The Directive clarifies that the Internal Market principle of mutual recognition of national laws and the **principle of the country of origin** must be applied to Information Society services. This will ensure that such services provided from another Member State are not restricted. The Directive does not deal with the application of the Brussels Convention on jurisdiction, recognition and enforcement of judgements in civil and commercial matters. The Directive does not interfere with the Rome Convention as regards the law applicable to contractual obligations in consumer contracts or with the freedom of the parties to choose the law applicable to their contract.

On a case by case basis, Member States will be allowed under the Directive to impose restrictions on Information Society services supplied from another Member State if necessary to protect the public interest on grounds of protection of minors, the fight against hatred on grounds of race, sex, religion or nationality, including offences to human dignity concerning individual persons, public health or security and consumer protection including the protection of investors.

However, such restrictions will have to be proportionate to their stated objective. Moreover, such restrictions can only be imposed (except in cases of urgency and in cases of court actions) after the Member State where the service provider is established has been asked to take adequate measures and failed to do so and the intention to impose restrictions has been notified in advance to the Commission and to the Member State where the service provider is established.

In cases of urgency and in cases of court actions, including preliminary proceedings and criminal investigations, the reasons for the restrictions (and the urgency) will have to be notified in the shortest possible time to the Commission and to the Member State of the service provider. Where the Commission considers proposed or actual restrictions are not justified, Member States will be required to refrain from imposing them or urgently put an end to them.

2.1.7. Relevance of Directives and Decisions to the EID concept

Not all of these aforementioned directives and decisions have direct impact on the data protection aspects of the EID concept. Some directives relate directly to the protection of personal data, i.e. the Directive 95/46 EC, the Directive 97/66 EC, the Directive 01/45 EC and the Decision 01/497, whereas the other Directives refer to the regulation of different topics, e.g. electronic signatures and electronic commerce, but refer to the data protection directives, especially to the Directive 95/46 EC.

In addition to that Directive, the Decision of the Commision 01/497 EC on standard contractual clauses has to be closely linked to that perspective as this Decision ensures adequate safeguards for personal data transferred from the EU to countries outside the Union.

As the EID concept will include electronic signatures based on PKI the data protection provision in the Directive 99/93 EC on electronic signatures has to be taken into account as well, as this regulation specifically deals with data protection issues relating to electronic signatures. The same relates to the Directive 00/31 EC on e-commerce.

Although the Directives 97/66 EC on data protection in telecommunications and 01/45 on data protection of the Community implement data protection issues, their relevance for the data protection issues directly related to the EID concept are of minor importance to the mission of this study.

However it has to be noted that, especially in the telecommunications area, the regulations of the Directive 97/66 EC will have to be studied as soon as the mobile device as a smartcard reader comes into the focus of the EID concept.

3. Data protection and the EID concept

From a data protection perspective the Directive 95/46 EC has to be identified as the main reference regulation for the EID concept. This Directive contains inter alia the basic principles for data protection, it defines personal data, the responsible entities, mandates Member States to implement technical security and regulates the data subject's rights and sets up a supervisory system.

3.1. Directive 95/46 EC and the EID concept

To assess the legal requirements of the Directive 95/46 EC for the EID concept it is necessary to give a short overview on the regulations of the Directive at stake and then, to discuss the implications for the EID concept.

3.1.1. Scope of the Directive 95/46 EC

The Directive 95/46 EC contains the general principles for processing of personal data within the European Union and regulates the transfer of personal data to third countries outside the European Union. However, although the Directive aims to harmonize data protection in the European Union as a whole, some important areas, which might affect the EID, are not within the scope of the European Directive.

3.1.1.1. General scope and applicable law, Article 3 and Article 4

Following Article 3 of the Directive, the Directive applies to the processing of personal data wholly or partly by automatic means, and to the processing otherwise than by automatic means of personal data which form part of a filing system or are intended to form part of a filing system. The Directive does not apply to the processing of personal data:

- in the course of an activity which falls outside the scope of Community law, such as those provided for by Titles V and VI of the Treaty on European Union and in any case to processing operations concerning public security, defence, State security (including the economic well-being of the State when the processing operation relates to State security matters) and the activities of the State in areas of criminal law,
- by a natural person in the course of a purely personal or household activity.

Each Member State has (Article 4) to apply the national provisions it adopts pursuant to this Directive to the processing of personal data where:

- the processing is carried out in the context of the activities of an establishment of the controller on the territory of the Member State; when the same controller is established on the territory of several Member States, he must take the necessary measures to ensure that each of these establishments complies with the obligations laid down by the national law applicable;
- the controller is not established on the Member State's territory, but in a place where its national law applies by virtue of international public law;
- the controller is not established on Community territory and, for purposes of processing personal data makes use of equipment, automated or otherwise, situated on the territory of the said Member State, unless such equipment is used only for purposes of transit through the territory of the Community.

The Directive refers to the public as well as to the private sector.

Member States have to determine more precisely the conditions under which the processing of personal data is lawful within their own jurisdiction. However they have to watch the limits of the provisions for the lawfulness of the processing of personal data.

3.1.1.2. EID concept

It is obvious that the EID as a concept will affect the automatic processing of personal data and that the concept as such is within the general scope of the Directive according to Article 3 paragraph 1.

The EID concept aims to build a universally recognized electronic ID token for identifying citizens in multiple use case scenarios. The EID will make it possible to pass the identity, once issued from one legal entity into other existing infrastructures of applications, whether in the public or the private sector. To issue the ID token it will be necessary to collect, store and process personal data. The EID concept will lead therefore to a processing of personal data by automatic means, whereby data are either processed on the EID card itself or will be closely linked to the automatic processing of personal data outside the EID card using various databases. In any case, the EID card will be connected to the processing of personal data by automatic means.

The EID concept will lead to automatic data processing by public and/or private organisations. This makes it easier to assess the usage scenarios for the different sectors by following the same requirements for pubic and private sector. However it has to be recognized that the scope of the Directive does not apply according to Article 3 paragraph 2 if the EID concept leads to a processing of personal data which is outside the activities of the Community or if the processing of personal data is purely done for personal purposes. As soon as the EID concept will be used in an area outside the scope of the Community law, the scope of the Directive is exempted. This relates especially to areas which are reserved to national legislation, e.g. public security, defence, State security and the activities in criminal law. The same applies if the EID card is used for purely personal or household activities.

The Directive mandates, according to Article 4, the Member States to apply the national provisions pursuant to the Directive in specific circumstances, mainly to prevent a conflict of law or a conflict of different jurisdictions, depending on where the data controller has its establishment, and to prevent the circumvention of the Directive's provisions. The main principle is that any processing of personal data in the Community must be carried out in accordance with the law of one of the Member States.

This will affect the EID concept as the EID token will bear one single identity which can be used throughout the European Union with various data controllers, processors or third parties having their establishments in one or more Member States.[10]

Processing of personal data carried out under the responsibility of a controller[11] who is established in a Member State has to be governed by the law of that Member State. Each data controller within the EID concept therefore has to comply with the national data protection provisions pursuant to the Directive. The same principle applies for a data controller having several establishments in different Member States. Establishment on the territory of a Member State implies the effective and real exercise of activity through stable arrangements. The legal form of such an establishment, whether simply a branch or a subsidiary with a legal personality, is not the determining factor in this respect.

When a single data controller within the EID concept is established on the territory of several Member States, particularly by means of subsidiaries, he must ensure, in order to avoid any circumvention of national rules, that each of the establishments fulfils the obligations imposed by the national law applicable to its activities.

If the processing of personal data is carried out by a data controller in a third country outside the European Union but using equipment situated in a Member State, the provisions of the Member State have to be applied to guarantee the protection of the individuals provided for in the Directive.

Independent of the decision on who is determining the purposes and means of the processing of personal data it has to be noted for the EID concept, that this principle is of high practical importance and affects organisational issues of the data controller. If the data controller is one entity or organisation the national data protection laws which have to be applied, are those where this data controller has its establishment. If the EID concept plans to have several distributed data controllers, the concept has to take into account that several national implementations of the Directive have to be in place. Under these circumstances it is desirable that the same data protection rules apply for all data controllers in whatever Member State they have establishments.

The Member States have to determine more precisely the conditions under which the processing of personal data is lawful within their own jurisdiction.[12] In most cases the roles of the different sectors are clearly defined in their specific areas of national regulations and thus the legal requirements follow the specific national legislation and the existing national legal organisational framework; e.g. the various European Member States have national data protection legislation matching the national legal environment. Although the European Directive 95/46 EC aims for harmonisation in European data protection, the differences in the various national data protection laws might be significant, e.g. the use of codes of conducts are in some Member States accepted, in other Member States they are not yet accepted.

3.1.2. Definitions

The Directive 95/46 EC defines in Article 2 the key words and functions which are referred to within the provisions of the Directive. The definitions follow the vocabulary of data protection legislation. They are especially important in defining the duties and obligations within the EID concept.

[10] See FIGURE 1.

[11] The role of the data controller is discussed in 3.1.2.2. in more detail.

[12] see Annex 1 for details of the national legislations in the European Union.

3.1.2.1. Key definitions of the Directive

The Directives provide some key definitions in the context of the protection of personal data which are used within the community framework to identify the obligations and responsibilities of the various parties participating in the processing of personal data.

- **Personal data** mean any information relating to an identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity;

- **Processing of personal data** means any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction;

- **Personal data filing system** means any structured set of personal data which are accessible according to specific criteria, whether centralized, decentralized or dispersed on a functional or geographical basis;

- **Controller** means the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data; where the purposes and means of processing are determined by national or Community laws or regulations, the controller or the specific criteria for his nomination may be designated by national or Community law;

- **Processor** means a natural or legal person, public authority, agency or any other body which processes personal data on behalf of the controller;

- **Third party** means any natural or legal person, public authority, agency or any other body other 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** means a natural or legal person, public authority, agency or any other body to whom data are disclosed, whether a third party or not; however, authorities which may receive data in the framework of a particular inquiry shall not be regarded as recipients;

- **The data subject's consent** means any freely given specific and informed indication of his wishes by which the data subject signifies his agreement to personal data relating to him being processed.

3.1.2.2. EID concept

The EID concept aims to build a universally recognized electronic ID token for identifying citizens in multiple use case scenarios. The EID will make it possible to pass the identity, once issued from one legal entity into other existing infrastructures of applications in either the public or the private sector.[13]

[13] See FIGURE 1

To issue the EID it will be necessary to collect, store and process **personal data** at various levels or steps: identification and registration of the card holder, issuance of certificates, provision of applications to the card holder and provision of services (content) to the card holder. The EID token may carry additional information or personal data on the card itself. Personal data will be either processed on the EID card itself or will be closely linked to the automatic processing of personal data outside the EID card using various databases.

Within the EID concept it has to be discussed whether the processing of personal data takes place on the card itself or outside the card; this may have a possible effect on the definition and accordingly on the responsibility for the various data protection provisions which are imposed on the **data controller** as the main responsible organisation or entity or agency for the protection of personal data. In this context it has to be discussed furthermore what roles the various parties within the EID concept will have from a data protection perspective.

This discussion has to take into account the specific functionalities of a smart card, which can be described as follows:

"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."[14]

This implies that the smart card offers a range of opportunities to perform operations upon personal data, either on board of the "pocket size computer" or outside the smart card, but in connection with the smart card. The most important question therefore is: Who is in control of these operations? The data subject himself and/or one organisation (private or public) or multiple organisations which can address the functionalities of the smart card ?

The data controller is a natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data.

From that point of view it has to be discussed within the EID concept who is determining – from a functional point of view - the purposes and means of the processing of personal data. It could be the data subject himself, the "smart card manufacturer", the "card issuer", the "application provider"[15] or any other organisation.

The data are not, or at least not mainly, controlled by the "data subject", as he is not determining the purposes and means of the smart card. Although he might have the possibility to view data stored on the card in using a suitable card reading facility, the data subject will not influence any of the computing processes relating to the processing of personal data.

[14] Rules of Conduct for Privacy and Card Intgrity, p. 6/7

[15] Rules of Conduct for Privacy and Card Integrity, p. 10

The data are also not controlled by the "smart card manufacturer", as he will only provide the smart card to the card issuer and will only provide the computational functionalities concerning the allocation and possible separations of different applications on the chip. He will not control the processing of personal data itself.

Possible data controllers, however, could be the "card issuer", the "application provider" and/or any organisation which builds on the smart card functionalities by processing personal data, e.g. offering services and content to the card holder.

The "card issuer" is the party that issues the card to the card holder, i.e. the data subject, and is responsible for the card management activities during the entire life cycle of the card. This process will be linked to the processing of personal data of the card holder, e.g. name, address, identity number, age, etc. at least for the purpose of issuing the card to the data subject.

The "card application provider" is the party offering an application system in which a smart card is used and who takes final responsibility for the proper functioning of the application. An application could be a transport service, a communication service, a payment service, medical services etc. Personal data will be processed in all these examples by connecting the card holder to a specific application, which is purchased with a specific application provider.

Last but not least, the "content provider" or the "service provider" has to be added to this list of possible data controllers. The content provider is the private or public organisation or entity which is delivering a specific service to the card holder, and which needs in turn personal data from the card holder.

In conclusion, the EID concept has to take into account that it is not possible to nominate one single data controller, but it has to recognize that several possible data controllers are at stake: the card issuer, the application provider and the content or the service provider.

It is therefore recommended that at least the "content or service provider" are included in any data protection provision within the EID concept. [16]

- "Content provider/service provider" means a natural or legal person, public authority, agency or any other body delivering a specific content or service to the card holder.

In addition to the above discussed roles of the "data subject" and the "data controller" the Directive 95/46 EC identifies the roles of the "processor", the "third party" and the "recipient". It is also recommended to add these roles to the data protection provision within the EID concept:[17]

- "Processor" means a natural or legal person, public authority, agency or any other body which processes personal data on behalf of the controller;

- "Third party" means any natural or legal person, public authority, agency or any other body other 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" means a natural or legal person, public authority, agency or any other body to whom data are disclosed, whether a third party or not.

[16] The role of the "content provider"/"service provider" should be included in the Code of Conduct accordingly.

[17] These roles should be identified in the Code of Conduct accordingly..

3.1.3. General rules for lawful processing of personal data

Chapter 2 (Articles 5 – 21) of the Directive 95/46 EC holds the most important provisions and regulations for the lawfulness of processing of personal data.

Following the general layout of the Directive it has to be noted that the provisions contained in this chapter have to be implemented by the Member States and that the implementation might have variations from one Member State to another.

The main principles to be mentioned within the EID concept are the principles of data quality, the principles for processing personal data lawfully, the data subject's rights and the principle of confidentiality and security of processing.

3.1.3.1. General rules of the Directive

3.1.3.1.1. Data quality, Article 6

According to Article 6 of the Directive 95/46 EC Member States have to provide that personal data must be:

- processed fairly and lawfully;
- collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes. Further processing of data for historical, statistical or scientific purposes shall not be considered as incompatible provided that Member States provide appropriate safeguards;
- adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed;
- accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that data which are inaccurate or incomplete, having regard to the purposes for which they were collected or for which they are further processed, are erased or rectified;
- kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the data were collected or for which they are further processed. Member States shall lay down appropriate safeguards for personal data stored for longer periods for historical, statistical or scientific use.

The controller has to ensure that data quality is guaranteed.

3.1.3.1.2. Criteria for legitimate data processing, Article 7 and Article 8

Article 7 of the Directive 95/46 EC describes the general conditions for the processing of personal data. Data controllers are required to observe several principles. These principles not only aim at protecting the data subjects but are a statement of good business practices which contribute to reliable and efficient data processing. In principle personal data can be processed either if the data subject has given his informed consent or whenever the controller or a third party has a legitimate interest in doing so and this interest is not overridden by the interest of protecting the fundamental rights of the data subject, particularly the right to privacy. The provision aims to establish a reasonable balance in practice between the business interest of the data controllers and the need for privacy of data subjects.

The Directive imposes obligations on the data 'controller' (i.e. the person or body 'which determines the purposes and the means of the processing') both in the public and in the

private sector. A medical practitioner would normally be the controller of the data relating to the clients of his practice, a company would be the controller of the data processing relating to clients and employees, a sports club would control the data processing relating to its members and a public library controls the data processing relating to its users. When a particular data processing operation is mandated by law, the law may determine who the 'data controller' is.

Personal data may according to Article 7 be processed only if:

(a) the data subject has unambiguously given his consent; or
(b) processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract; or
(c) processing is necessary for compliance with a legal obligation to which the controller is subject; or
(d) processing is necessary in order to protect the vital interests of the data subject; or
(e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller or in a third party to whom the data are disclosed; or
(f) processing is necessary for the purposes of the legitimate interests pursued by the controller or by the third party or parties to whom the data are disclosed, except where such interests are overridden by the interests for fundamental rights and freedoms of the data subject which require protection under Article 1 (1).

In the case of **sensitive data**, the Directive establishes that such data can only be processed with the explicit consent of the individual, subject to a number of exemptions for specific cases such as consent of the data subject or where there is an important public interest (e.g. for medical or scientific research) where alternative safeguards have to be established. In the specific case of personal data used exclusively for journalistic, artistic or literary purposes, the Directive requires Member States to ensure appropriate exemptions and derogations exist which strike a balance between guaranteeing freedom of expression while protecting the individual's right to privacy.

Article 8 regulates the prohibition of processing of certain personal data. Especially the processing of special categories of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and the processing of data concerning health or sex life are prohibited under the Directive.

However this shall not apply where:

(a) the data subject has given his explicit consent to the processing of those data, except where the laws of the Member State provide that the prohibition referred to in paragraph 1 may not be lifted by the data subject's giving his consent; or
(b) processing is necessary for the purposes of carrying out the obligations and specific rights of the controller in the field of employment law in so far as it is authorized by national law providing for adequate safeguards; or
(c) processing is necessary to protect the vital interests of the data subject or of another person where the data subject is physically or legally incapable of giving his consent; or
(d) processing is carried out in the course of its legitimate activities with appropriate guarantees by a foundation, association or any other non-profit-seeking body with a political, philosophical, religious or trade-union aim and on condition that the processing relates solely to the members of the body or to persons who have regular

contact with it in connection with its purposes and that the data are not disclosed to a third party without the consent of the data subjects; or

(e) the processing relates to data which are manifestly made public by the data subject or is necessary for the establishment, exercise or defence of legal claims.

Furthermore Article 8 Paragraph 1 does not apply where processing of the data is required for the purposes of preventive medicine, medical diagnosis, the provision of care or treatment or the management of health-care services, and where those data are processed by a health professional subject under national law or rules established by national competent bodies to the obligation of professional secrecy or by another person also subject to an equivalent obligation of secrecy.

Processing of personal data relating to offences, criminal convictions or security measures may be carried out only under the control of official authority, or if suitable specific safeguards are provided under national law, subject to derogations which may be granted by the Member State under national provisions providing suitable specific safeguards. However, a complete register of criminal convictions may be kept only under the control of official authority.

Article 8 paragraph 7 leaves it up to the Member States to determine the conditions under which a national identification number or any other identifier of general application may be processed.

3.1.3.2. EID concept

Any processing of personal data within the EID concept has to follow the principles mentioned in Articles 6, 7 and 8 of the Directive. Together with the data subject's rights these provisions constitute the reference text (the "bible") for any information operation process within the EID concept.

3.1.3.2.1. EID concept and data quality

Any processing of personal data within the EID concept must be lawful and fair to the data subjects. In particular data within the EID concept must be adequate, relevant and not excessive in relation to the purposes for which they are processed; the purposes must be explicit and legitimate and must be determined at the time of collection of the data; the purposes of processing further to collection shall not be incompatible with the purposes as they were originally specified.

Within the EID concept personal data on identification will be collected and processed. These identification data will e.g. constitute the main reference data within the GIF model. Certification service providers will need to collect, store and process personal data which are identifiable. The Directive specifically mandates that these data are not stored for a longer period than necessary for the purposes for which the data were collected or for which they are further processed. This implies that within the EID concept it is necessary to clearly identify those cases where identification data are necessary and, if these data are no longer needed for the purposes of the data storage, what will happen to these data.

It is recommended that these major principles, which are implemented in all national data protection laws, should be mentioned explicitly in the Code of Conduct. It is the responsibility of each data controller to safeguard the data quality. Moreover the issue of identification of the data subject has to be addressed in the Code of Conduct.

3.1.3.2.2. EID concept and criteria for legitimate data processing

A smart card can be the "ultimate instrument"[18] or "The intelligent key to *e*-services"[19] 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. 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 and where data are collected on which occasion. This may be especially an issue when contactless cards can be read and updated from a distance without requiring direct action from the cardholder or even without the cardholder knowing.[20]

It is therefore mandatory that the collection, the storage and any other processing of personal data is in line with the requirements of the Directive 95/46 EC. In addition to the principles for data quality in Article 6 the Directive uses accepted principles to provide legitimacy to data processing:

- the consent of the data subject,
- the contractual relationship between the data subject and the data controller,
- a legal requirement,
- for the performance of a task carried out in the public interest or in the exercise of official authority,
- the legitimate interests of a natural or legal person, provided that the interests or the rights and freedoms of the data subject are not overriding.

According to Article 7 the processing of personal is only justified if these requirements are respected. It depends on each usage scenario what justification is appropriate for the processing of personal data within the EID concept. Within the EID concept it is necessary to implement these requirements for each usage scenario. It is not only in the interest of the data subject, but in the interest of companies and organisations to build on a sound basis for data processing. By discussing the different relationships between the data subjects and the various legal entities it should be possible to find justifiable processing scenarios.

Without any prejudice to the usage scenarios, the main guideline may be that within the EID concept it is most probable that private companies' processing of personal data may be justified by consent of the data subject or by contractual relationships, whereas public agencies' processing will be justified by legal requirements.

The consent of the data subject and the conclusion of a contractual relationship are the most obvious scenarios, as these two cases offer the data subject an informed decision on the processing of personal data.

However, the consent of the data subject is the best possible guarantee for wide acceptance of the use of smart cards, the applications and services. It has to be noted that the consent has different requirements in Article 7 and Article 8: "Consent" in Article 7 means that the data subject has given his consent "unambiguously", i.e. not explicitly but at least without any serious doubts. It requires an informed decision of the data subject taking into account the processing and the purposes of the processing of personal data. The mere use of a smart card would not be sufficient to count as "informed consent". In addition, in the case of processing sensitive data, Article 8 requires an "explicit" consent of the data subject. Data

[18] Code of Conduct, p. 7

[19] GIF part 2, p. 5

[20] Code of Conduct, p. 7

which are capable by their nature of infringing fundamental freedoms or privacy should not be processed unless the data subject gives his explicit consent.

It is recommended that the different usage scenarios, the sectors affected and the personal data necessary for processing are discussed in more detail as soon as usage scenarios are defined.[21]

One specific issue has to be addressed in the future discussion of the EID concept: The EID concept may lead to some kind of an identification number, e.g. by using a certificate, a pseudonym or any other identifier. This universal number would cause serious concern to data subjects as it would possibly allow the accumulation of personal data around the unique identifier, from various databases and eventually end in a personal profile.

The Directive addresses this issue in Article 8 paragraph 7, but leaves it up to the Member States to determine the conditions under which a national identification number or any other identifier of general application may be processed.

3.1.4. Confidentiality and security of processing of personal data

Confidentiality of the personal data while processed and security of the processing itself are a “must” when protecting the personal data of a data subject. Using a smart card within data processing with its many technical options is a challenge for these principles and, at the same time, an opportunity to provide a technically viable solution for safeguarding confidentiality and the security of the processing of personal data.

3.1.4.1. Confidentiality and security, Article 16 and Article 17

The Directive 95/46 EC implies two main principles: confidentiality, which is related to the processors of personal data (Article 16) and security which relates to the technical security of the processing itself (Article 17).

Any person acting under the authority of the data controller or of the data processor, including the processor himself, who has access to personal data must not process them except on instructions from the controller, unless he is required to do so by law.

Member States have to provide that the controller must implement appropriate technical and organizational measures to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.

Having regard to the state of the art and the cost of their implementation, such measures shall ensure a level of security appropriate to the risks represented by the processing and the nature of the data to be protected.

The Member States have to provide that the controller must, where processing is carried out on his behalf, choose a processor providing sufficient guarantees in respect of the technical security measures and organizational measures governing the processing to be carried out, and must ensure compliance with those measures.

[21] see Figure 1

The carrying out of processing by way of a processor must be governed by a contract or legal act binding the processor to the controller and stipulating in particular that the processor acts only on instructions from the controller, and the obligations for security measures shall also be incumbent on the processor.

Finally, for the purposes of keeping proof, the parts of the contract or the legal act relating to data protection and the requirements relating to the measures referred to in paragraph 1 shall be in writing or in another equivalent form.

3.1.4.2. EID concept

A smart card can be the "ultimate instrument"[22] or "The intelligent key to *e*-services"[23] 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. 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 and where data are collected on which occasion. This may be especially an issue when contactless cards can be read and updated from a distance without requiring direct action from the cardholder or even without the cardholder knowing.[24]

The EID concept has to watch these two principles very carefully. Any threat of unwanted disclosure of personal data on the smart card or from a database will question the reliability of the card itself and thus reduce acceptance of the technology with the data subject.

3.1.4.2.1. Confidentiality

First of all it has to be clearly defined who is responsible for the processing of personal data and who is processing the personal data on behalf of the data controller. The data controller has to make sure that the necessary confidentiality agreements are in place.

Once again the relationships and the responsibility of each entity involved in the processing has to be clarified from the very beginning: who is the data controller, who is the processor, and are the appropriate contractual relationships between the controller and the processor in place ?

3.1.4.2.2. Technical security

The protection of the rights and freedoms of data subjects with regard to the processing of personal data requires that appropriate technical and organizational measures are taken, both at the time of the design of the processing system and at the time of the processing itself, particularly in order to maintain security and thereby to prevent any unauthorized processing; it is up to the Member States to ensure that data controllers comply with these measures; these measures must 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 Directive leaves it to the Members States to define the right technical security measures. It does not exclude any technical device ex ante. The data controller will be responsible for

[22] Code of Conduct, p. 7

[23] GIF part 2, p. 5

[24] Code of Conduct, p. 7

direct security, which is under his own control, as well as for the indirect security measures, which are with the processor of personal data.

In assessing the right level of technical security within the EID concept it is necessary to assess all risks and the nature of personal data processed.

Risks for accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access will e.g. be higher if personal data are stored in circumstances where the data subject or the data controller cannot control the processing of personal data. This may happen if personal data are stored on the EID card itself. However this risk assessment depends on the type of personal data stored on the EID card (e.g. basic data versus medical data). The risks may be higher if contactless cards, which enable seamless communication between the card and the data controller, are involved. The risks may also be higher if biometric data are included in the processing.

The overall goal for the processing of personal data has to be to minimize the personal data required and to use the technical functions available to that end. This means e.g. anonymization of personal data and using pseudonyms for the data subjects whenever possible and technically feasible.

It is necessary to take these considerations into account in designing the EID concept. The GIF model infrastructure could support this risk assessment for the technical security by defining e.g.:

- what kind of personal data have to be stored on the EID card (minimum level),
- what kind of personal data may be stored in addition to these minimum personal data (maximum level),
- what compartments for what personal data are managed on the card,
- what computational processes with personal data can be done on the card,
- what computational processes relate to the data stored on the card,
- what are the links for processing personal data between the different parties.

As the Directive does not contain any specific catalogue for technical security of processing personal data it is, again, necessary to look into the legislation of member States for the national implementation of this principle. Some national legislation on data protection has taken these principles into account and mandated e.g. the minimization of processing of personal data in general.[25]

It would be desirable for the EID concept to have one overall security concept which would implement in general terms the required security features and thus would contribute to a harmonized approach for the EID concept.[26]

3.1.5. Data subject's rights

Data subjects are granted a number of rights within the Directive 95/46 EC and they may appeal to independent national authorities if they consider their rights are not being respected. These rights and the due execution of these rights have to be reflected within the EID concept.

[25] e.g. Federal Data Protection Legislation Germany, Article 3c

[26] The Code of Conduct refers to the security aspect in general terms only, Article 3. The catalogue however should be more consistent with the risks at stake.

3.1.5.1. Data subject's rights, Articles 10, 11, 12, 13, 14

Data subjects are granted a number of important rights. These rights include: information from subsequent data users about where the data originated (where such information is available), the identity of the organisation processing data about them and the purposes of such processing; a right of access to personal data relating to him/her; a right to rectification of personal data that is shown to be inaccurate and the right to opt out of allowing their data to be used in certain circumstances (for example, for direct marketing purposes, without providing any specific reason).

Each data controller has to comply with the provisions of the Member State where he is established even if the personal data relate to data subjects established in other Member States except where the controller is established in another Member State as well. In this case the law of the country of that establishment is applicable to its processing. When the data subject is not established in the Community (e.g. a foreign company) he has to comply with the law of the Member State(s) where the processing equipment (e.g. a computing centre) is located. Controllers established outside the Community are required to appoint a representative in the Community.

Data controllers are required to give information to the data subjects whenever they process personal data, unless the data subjects already have this information. Data subjects must be informed of the identity of the controller and of the purposes of the processing as well as in some circumstances of the categories of data involved, of the recipients of the data and of the specific rights of the data subjects.

Data subjects must receive this information both if the data are obtained from them or if they are obtained from third parties. Derogations may however apply in the latter case, when the giving of this information proves impossible or might involve a disproportionate effort.

3.1.5.2. EID concept

The "magna carta" of any data protection regulations are the rights of the data subject. These rights enable the data subject to have transparency on the processing of personal data, they enable the data subject to judge the purposes of any processing of his personal data, to view stored personal data and to reject unlawful processing. At the same time the correct execution of these rights put the obligation on the data controller to inform the data subject of any processing step. This information is the basis for the trust relationship between the data subject and the data controller.

The use of smart cards provides a way of both increasing and decreasing transparency. 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 his 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.[27]

3.1.5.2.1. Information to the data subject, Article 10 and Article 11

[27] Code of Conduct, p. 6

The data subject must be in a position to learn of the existence of a processing operation and, where data are collected from him, must be given accurate and full information, bearing in mind the circumstances of the collection. Any person must be able to exercise the right of access to data relating to him which are being processed, in order to verify in particular the accuracy of the data and the lawfulness of the processing; every data subject must also have the right to know the logic involved in the automatic processing of data concerning him.

Article 10 of the Directive therefore mandates that the following information be given by the data controller to the data subject if the data controller collects data from the data subject:

(a) the identity of the controller and of his representative, if any;
(b) the purposes of the processing for which the data are intended;
(c) any further information such as
    i. the recipients or categories of recipients of the data,
    ii. whether replies to the questions are obligatory or voluntary, as well as the possible consequences of failure to reply,
    iii. the existence of the right of access to and the right to rectify the data concerning himin so far as such further information is necessary, having regard to the specific circumstances in which the data are collected, to guarantee fair processing in respect of the data subject.

Article 11 of the Directive mandates the same information in cases where the data controller has not collected personal data directly from the data subject. In that case the data controller has to inform the data subject when the data are recorded or, at the latest, when the data are first disclosed to a third party in so far as such further information is necessary, having regard to the specific circumstances in which the data are processed, to guarantee fair processing in respect of the data subject:[28]

(a) the identity of the controller and of his representative, if any;
(b) the purposes of the processing;
(c) any further information such as
    i. the categories of data concerned,
    ii. the recipients or categories of recipients,
    iii. the existence of the right of access to and the right to rectify the data concerning him

Within the EID concept each data controller has to follow these requirements for information. To increase the acceptance of the EID card it is recommended that the data controllers aim at giving at least the required information pursuant to the Directive. They are however free to give more information.[29]

However, it has to be noted that the necessary information has to be provided by either the card issuer, the application provider and/or the content or service provider. Within the EID concept this situation could lead to a multiple information exercise, which is leading more to confusion with the data subject than to transparency. It would be desirable to concentrate the required information on one specific data controller, which could be the card issuer.[30] As long as the intended processing of personal data is known, this “combined information” to the data subject is a reasonable way of handling the required information. Nevertheless, this simplification will not relieve any other content or service provider who is added later on to the EID framework from his obligations on information.

[28] This obligation should be clarified in the Code of Conduct. So far the Code of Conduct only refers to information given to the card holder/data subject prior to collection of personal data by the card issuer.

[29] The Code of Conduct enlarges the information necessary, see Article 7 and 8.

[30] This seems to be the intention of the Code of Conduct in Article 7.

3.1.5.2.2. Rights to access, rectification, erasure and blocking, Article 12

Every data subject has the right to obtain from each data controller confirmation as to whether or not data relating to him are being processed and information at least as to the purposes of the processing, the categories of data concerned, and the recipients or categories of recipients to whom the data are disclosed, and communication to him in an intelligible form of the data undergoing processing and of any available information as to their source.

Every data subject has the right to rectification, erasure or blocking of data the processing of which does not comply with the provisions of this Directive, in particular because of the incomplete or inaccurate nature of the data.

Finally the data subject has the right of notification to third parties to whom the data have been disclosed of any rectification, erasure or blocking carried out unless this proves impossible or involves a disproportionate effort.

The EID concept has to enable the execution of these rights without any constraint and without excessive delay or expense.[31] The use of the EID card for accessing this information online should be appropriate.[32]

3.1.5.2.3. Right to object, Article 14

According to Article 14 the data subject has the right to object to certain processing of personal data. The data subject should have the right to object at any time on compelling legitimate grounds relating to his particular situation to the processing of data relating to him and in particular 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 purposes of direct marketing, or to be informed before personal data are disclosed for the first time to third parties or used on their behalf for the purposes of direct marketing, and to be expressly offered the right to object free of charge to such disclosures or uses.

Again, the EID concept has to take due account of this right to object.[33]

3.1.6. Notification, Articles 18 and 19

In order to ensure that the public are properly informed about data processing operations and also so as to allow the supervisory authorities to perform their tasks, the directive devises a system of notification for processing operations. National data protection authorities are required to keep a public register indicating details of the data controllers and of the processing undertaken.

Member States may provide for simplification or exemption from notification for specific types of processing operations which do not entail particular risks (often the most common types) Exception and simplification can also be granted when an independent officer in charge of

[31] The Code of Conduct refers to these rights in Articles 16 and 17.

[32] The Code of Conduct mentions a "written" procedure, which should not be the case if the usage of the card is possible and will facilitate the execution of the rights to access etc.

[33] The Code of Conduct refers to the right to object only in the case of direct marketing, Article 18.

data protection within the organisation processing data has been appointed in conformity with national law.

Member States may require prior checking to be carried out by the supervisory authority before data processing operations in cases involving particular risks may be undertaken.

To enable proper supervision of the processing of data the EID concept should imply the notification procedure. It is recommended that this notification procedure is added to the Rules of Conduct.

3.1.7. Codes of conduct

The EID concept aims at building a universal framework for the eSSC constituency. To be effective this framework has to recognized by the industry itself and by the responsible authorities. Member States and the Commission, in their respective spheres of competence, are encouraging especially trade associations and other representative organizations concerned to draw up codes of conduct to facilitate the application of the Directive 95/46 EC, taking account of the specific characteristics of the processing carried out in certain sectors, and respecting the national provisions adopted for its implementation. A code of conduct in respect to the EID concept can therefore be an accepted instrument to handle the data protection issues related to the EID concept.

3.1.7.1. Codes of conduct, Article 27

According to Article 27 of the Directive 95/46 EC the Member States and the Commission shall encourage the drawing up of codes of conduct intended to contribute to the proper implementation of the national provisions adopted by the Member States pursuant to this Directive, taking account of the specific features of the various sectors. Codes of conduct can be implemented either on the national level of each Member State or they can be implemented at the Community level.

Member States may make provision for trade associations and other bodies representing other categories of controllers which have drawn up draft national codes or which have the intention of amending or extending existing national codes to be able to submit them to the opinion of the national authority. Member States shall make provision for this authority to ascertain, among other things, whether the drafts submitted to it are in accordance with the national provisions adopted pursuant to this Directive. If it sees fit, the authority shall seek the views of data subjects or their representatives.

Community codes, or amendments to already existing codes of conduct on the Community level, may be submitted to the Working Party referred to in Article 29 of the Directive. This Working Party shall determine, among other things, whether the drafts submitted to it are in accordance with the national provisions adopted pursuant to this Directive. If it sees fit, the authority shall seek the views of data subjects or their representatives. The Commission may ensure appropriate publicity for the codes which have been approved by the Working Party.

3.1.7.2. EID concept

The EID concept aims at building a universal framework for the eSSC constituency. To be effective this framework has to recognized by the industry itself and by the responsible authorities. A code of conduct in respect to the EID concept can therefore be an accepted instrument to handle the data protection issues related to the EID concept.

This Code of Conduct for EID would 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.[34]

The Code of Conduct for EID related data protection is therefore a valuable and accepted contribution from the Directive's point of view. In addition, it would help to overcome to a certain extent the need to match the EID concept not only to the Directive but also to the implementation of the data protection legislation in Member States. The Code of Conduct will be "soft law" and it has to be matched against all implementations of the Member State or the Member States. It does not replace the national legislation, but it could support initiating such kind of legislation in the Member States.

As regards ossible procedures, Article 27 states that a Code of Conduct can be either initiated at the level of one Member State[35] or at the Community level. Taking into account the already established European wide activity of the eESC it would be reasonable to start with a Code of Conduct at the Community level. However it is also possible to start the initiative in one or two members States and after acceptance to bring it to the Community level.

The initiative should be started by "trade associations and other bodies representing other categories of controllers which have drawn up draft national codes or which have the intention of amending or extending existing codes to be able to submit them to the opinion of the Commission". This could be done e.g. by the European Chamber of Commerce or other similar organisations – the "eESC constituency"[36] should have at least the opportunity to initiate such Code of Conduct, maybe together with other established organisations. The Directive does not indicate any specific requirements for this.[37]

The Code of Conduct should then be addressed to the Working Party referred to in Article 29 ("Working Party"). The "Working Party on the Protection of Individuals with regard to the Processing of Personal Data" has an advisory status and acts independently. The Working Party is composed of a representative of the supervisory authority or authorities designated by each Member State and of a representative of the authority or authorities established for the Community institutions and bodies, and of a representative of the Commission. The Working Party takes decisions by a simple majority of the representatives of the supervisory authorities.

Decisions on Codes of Conduct at the Community level will have to take into account the data protection regulations of the Member States, i.e. the Working Party will have to match the proposed Code of Conduct to each Member State where it is intended it will be applied. The EU Commission is authorised to publish the Code of Conduct, as soon as the Working Party has approved the Code of Conduct.

---

[34] Code of Conduct, p. 8

[35] Codes of conduct are already accepted in the Netherlands and in Ireland, whereas both member States have different legal traditions.

[36] Code of Conduct, p. 9

[37] It is also possible that the Working Party may, on its own initiative, make recommendations on all matters relating to the protection of persons with regard to the processing of personal data in the Community, Article 30 paragraph 3.

In relation to the “Rules of conduct for privacy and card integrity” it is therefore recommended to match the rules to the national data protection rules pursuant to the Directive and for these rules to be proposed to the Working Party by an appropriate industry association.

3.1.8. Transfer of personal data to third countries

The EID aims to build a universally recognized electronic ID token for identifying citizens in multiple use case scenarios. The EID will make it possible to pass the identity, once issued, from one legal entity into other existing infrastructures of applications, whether in the public or the private sector. In addition the EID will use certification service providers, most probably in different national legislations.

3.1.8.1. Transfer of personal data to third countries, Article 25 and Article 26

For cases where data is transferred to non-EU countries, the Directive includes provisions to prevent the EU rules from being circumvented in Article 25 and Article 26.

The basic rule is that the data should only be transferred to a non-EU country if it will be adequately protected there, although a practical system of exemptions and special conditions also applies (such as for data where the subject has given consent or which is necessary for performance of a contract with the person concerned, to defend legal claims or to protect vital interests (e.g. health) of the person concerned).

Such provisions are compatible with the General Agreement on Trade in Services (GATS, Article XIV), which recognises the protection of personal data as a legitimate reason for restricting the free movement of services. The advantage for non-EU countries where adequate protection can be provided is that the free flow of data from all 15 EU states will henceforth be assured, whereas up to now each Member State has decided on such questions separately. The adequacy of data protection safeguards concerning transfers to non-EU countries will be considered case by case. Adequacy will not necessarily require a non-EU country to apply legislation similar to the EU's Directive.

Alternative systems, such as voluntary arrangements applied by industry, or binding contractual clauses between the parties concerned in the data transfer, may be considered adequate if they are effectively applied and offer sufficient safeguards concerning data subjects' rights, including rights of redress.[38]

Under the Directive, if a Member State's data protection authorities considered a particular set of data would not be adequately protected if transferred to a non-EU country, they could block the individual data transfer, but not all transfers of data to the country concerned. The national authorities would have to inform the Commission, which would inform all other Member States. If the Commission and all other Member States agreed that the decision was justified, it would be extended to the EU as a whole. Otherwise, the decision would be overturned. In other words, a decision to block a transfer of data to a non-EU country applies across the EU as a whole or not at all.

A committee of Member State officials established under the Directive (Article 31) considers issues arising from data transfers to third countries.[39]

The Commission is involved in on-going contacts with a number of non-EU countries in order to explore ways of avoiding possible interruptions to exchanges of personal data.[40] The

[38] The model clauses are specificly referred to by the Decision 01/497 EC; see 3.1.8.2. for details.

[39] The Commission shall be assisted by a committee composed of the representatives of the Member States and chaired by the representative of the Commission; this Committee is different from the Working Party according to Artcile 29.

[40] The “Safe Harbor” principles with the US are one result of these considerations.

Article 31 Committee meets regularly to consider the current state of play on these contacts and consults with the Working Party according to Article 29, which is to give its opinion on the level of data protection in third countries.

3.1.8.2. EID concept

The EID concept aims at a cross-industry framework, where personal data may be transferred from one company to another company or from one government agency to another government agency not only within the European Union, but also to non-EU countries. From that perspective special attention should be paid to the data transfer to non-EU countries which do not have an adequate level of protection for personal data.

However before entering into a discussion on a model contract within the EID concept on data transfer to non-EU countries, the following questions have to be answered:

1. What are the main countries outside the scope of the Directive 95/46 EC ?
2. What data protection level do these countries offer ?
3. Does this data protection level match the provisions of the Directive 95/46 EC in a sense that these provisions may be considered adequate ?
4. Do these countries have accepted business rules accepted by the Article 31 Committee ?
5. In case these data protection provisions are not to be considered as adequate, and in case there are no other model contracts applying, can transfers take place under the provisions of Article 26 ?
6. Last but not least, what model contract could be the right instrument to guarantee the adequacy of data protection ?

It has to be noted, that even where it is found that there is not adequate protection, transfers may take place in circumstances specified in Article 26. This will be the case when, for example:

- the individual has given his unambiguous consent to the transfer, or
- the transfer is necessary for the performance of a contract with the individual concerned (e.g.: employment contracts) or the implementation of pre-contractual measures taken in response to his/her request (e.g.: application for a job), or
- the transfer is necessary or legally required for the establishment, exercise or defence of legal claims, or
- the transfer is necessary in order to protect the vital interests of the individual (e.g.: transfer of medical data concerning an individual hospitalised in a non-EU country).

Other exceptions are provided by the Directive and show that, even for data flows to those countries which do not ensure an adequate level of protection, there are a number of “bridges”. For some of these bridges, the key is held by the data subject, i.e his consent.

Where this condition is not met, the bridge can be built by the industry itself. In that sense a “EID Model Contract”[41] could help to ensure the acceptance of the transfer of data to non-EU countries. Therefore the EID concept may establish safeguards that make them less dependent on the good will of the legislators of a given country. Even in the best case scenario, a number of non-EU countries are likely to fall short of an "adequate" level of protection, and individuals may be reluctant to give their consent to the transfer to such countries of their personal data. In addition this “EID Model Contract” would speed up the

[41] The Working Group according to Article 29 has already adopted a document giving guidance on the role of contracts generally, which could be used.

process with multiple private companies and/or public agencies. This standard “EID Model Contract” could be an integral or an annexed part of the Code of Conduct.

This contract, however, would not be authorised by one Member State (see Article 26 paragraph 2), as this “EID Model Contract” would relate to multiple usage scenarios and multiple companies and/or agencies in non-EU countries. It would be necessary to have the “EID Model Contract” accpeted by the Commission in accordance with the procedure in Article 31 as a standard contractual clause for data transfers within the EID concept.

3.2. Decision on model clauses 01/497 EC and the EID concept

The Commission encourages the use of model contracts when personal data are to be transferred to non-EU countries.

The standard contractual clauses contain a legally enforceable declaration ("warrant") whereby both the "Data Exporter" and the "Data Importer" undertake to process the data in accordance with basic data protection rules and agree that individuals may enforce their rights under the contract.

The Commission Decision obliges Member States to recognise the contractual clauses annexed to the Decision[42] as providing adequate safeguards and fulfilling the requirements of the Directive for data transfers to non-EU countries that do not provide for an adequate level of protection for personal data. However, the standard contractual clauses are neither compulsory for businesses, nor are they the only way of lawfully transferring data to third countries. They add a new possibility to those already existing under the Data Protection Directive, which establishes several cases where data may still be transferred to countries where the data protection regime is not adequate. These include cases where individuals have given their unambiguous consent for data to be transferred outside the EU and where the transfer is necessary for the conclusion or performance of a contract in the interest of the data subjects. In addition, Member States’ data protection authorities may authorise such transfers on a case by case basis when they are satisfied the data enjoys "adequate protection".

Contractual clauses are not necessary for the transfer of data to Switzerland or Hungary, whose own data protection regimes have been recognised by the Commission as offering adequate protection, or to US companies adhering to the ‘Safe Harbor’ Privacy Principles issued by the US Department of Commerce.[43]

Data Protection Authorities in the Member States retain powers to prohibit or suspend data flows in exceptional circumstances, but the effect of this Decision is that they cannot refuse data transfers made under contracts that incorporate the standard contractual clauses approved by the Commission. The Decision also does not prevent national Data Protection Authorities authorising other *‘ad hoc’* contractual arrangements for the export of data out of the EU based on national law, as long as these authorities are satisfied that the contracts in question provide adequate protection for data privacy.

This Decision is only a first step in developing contractual solutions as a tailor-made tool for the transfer of personal data world-wide. The Commission intends to adopt separate

[42] Further information about this Decision and the standard contractual clauses, including exchanges of letters with business associations and the US Departments of Commerce and Treasury http://europa.eu.int/comm/internal_market/en/dataprot/news/index.htm

[43] see working documents of the Working Group Article 29, June 2002 http://europa.eu.int/comm/internal_market/en/dataprot/news/index.htm

Decisions referring to specific types of transfers and situations. The Commission is consulting Member States and Data Protection Authorities on a new draft Decision concerning standard contractual clauses for the transfer of personal data from data controllers established in the Community to data processors established in non-EU countries.

The harmonisation of data protection rules in the EU aims to ensure the free movement of information (including personal data) between Member States, whilst at the same time ensuring a high level of protection for any person concerned. In the case of non-EU countries, Directive 95/46 EC requires Member States to permit transfers of personal data only where there is "adequate protection" for such data, unless one of a limited number of specific exemptions applies. Without such rules, the high standards of data protection established by the Directive could be quickly undermined, given the ease with which data can be moved around using international networks.

- The Directive requires the following general principles to be applied:
    - personal data should be collected only for specified, explicit and legitimate purposes
    - the persons concerned should be informed about such purposes and the identity of the data controller
    - any person concerned should have a right of access to his/her data and the opportunity to change or delete data which is incorrect and
    - if something goes wrong, appropriate remedies must be available to put things right, including compensation or damages through the competent courts.

3.3. Directive 99/93 EC on electronic signatures and data protection

The European Union has issued the European Electronic Signature Directive, and the individual Member Countries have implemented this framework into national law. European countries that are not yet in the EU are following. The same holds true for the Americas. In the US, for instance, the patchwork of different state laws has been unified on important points through a federal law that puts electronic signatures on equal footing with their pen-and-ink counterparts in most types of business transactions. Most Asian and Asian-Pacific countries (including Singapore, Korea, Malaysia, Hong Kong, India and Japan) already have legislation on electronic signatures in place.

This legislative environment offers a foundation upon which the EID concept can build.[44]

3.3.1. Data protection provision

Specific data protection provisions may be included in European Directives which regulate specific areas. The Directive 99/93 EC has one specific provision on data protection concerning the processing of personal data by certification service providers.

According to Article 8 paragraph 1, Member States have to ensure that certification-service-providers and national bodies responsible for accreditation or supervision comply with the requirements laid down in the Directive 95/46 EC.

Article 8 paragraph 2 adds the obligation of Member States to ensure that a certification-service-provider which issues certificates to the public may collect personal data only directly from the data subject, or after the explicit consent of the data subject, and only insofar as it is necessary for the purposes of issuing and maintaining the certificate. The personal data may not be collected or processed for any other purposes without the explicit consent of the data subject.

Article 8 paragraph 3 Member States shall not prevent, without prejudice to the legal effect given to pseudonyms under national law, certification service providers from indicating in the certificate a pseudonym instead of the signatory's name.

3.3.4. EID concept

The EID concept will deal with electronic signatures and will therefore set up relationships between the data subjects and certification-service providers. According to Article 2 lit. 11 of the Directive on electronic signatures certification-service provider means an entity or a legal or natural person who issues certificates or provides other services related to electronic signatures.

Following the basic principle that the data protection Directive 95/46 provides the basic provisions for processing of personal data the certification-service provider has to follow these provisions. Insofar as the certification–service provider acts as the data controller he has to follow all provisions which have been described in the context of the Directive 95/46 EC.

[44] The EID concept will build on PKI. Details from a legal perspective of this Directive will not be discussed in this study, as it concentrates on the data protection aspects.

In addition to this more general provision the certification-service provider within the EID concept has to follow the specific data protection regulation pursuant to Article 8 of the Directive on electronic signatures by applying the personal data which may be collected and processed by the certification-service provider strictly to the purposes of issuing and maintaining the certificate. By this the personal data processed will be very limited, except the data subject explicitly consents to the processing for other purposes. It is recommended that this specific provision be taken into account in the Code of Conduct.

In addition to this strict purpose-orientation it has to be noted that the possible use of pseudonyms does not prevent Member States from requiring identification of persons pursuant to national or Community law.

3.4. Directive on e-commerce 00/31 EC

The Directive on a Legal Framework for Electronic Commerce Directive 2000/31/EC was adopted on 8th June 2000. Member States had 18 months in which to implement the Directive into national law following its publication in the EU's Official Journal. Most of the European member states had adopted the Directive's principles into the national regulatory framework by 17th January 2002.

The Directive covers all Information Society services, both business to business and business to consumer, and services provided free of charge to the recipient e.g. funded by advertising or sponsorship revenue and services allowing for on-line electronic transactions such as interactive tele-shopping for goods and services and on-line shopping malls. Examples of sectors and activities covered include on-line newspapers, on-line databases, on-line financial services, on-line professional services (such as lawyers, doctors, accountants, estate agents), on-line entertainment services such as video on demand, on-line direct marketing and advertising and services providing access to the World Wide Web.

3.4.1. Directive on e-commerce and data protection

The Directive on e-commerce does not contain any specific provision as regards data protection. The Directive considers that the protection of individuals with regard to the processing of personal data is solely governed by Directive 95/46/EC and the Directive 97/66/EC concerning the processing of personal data and the protection of privacy in the telecommunications sector. These Directives are fully applicable to information society services.[45]

These Directives already establish a Community legal framework in the field of personal data and therefore it is not necessary to cover this issue in this Directive in order to ensure the smooth functioning of the internal market, in particular the free movement of personal data between Member States; the implementation and application of this Directive should be made in full compliance with the principles relating to the protection of personal data, in particular as regards unsolicited commercial communication and the liability of intermediaries; this Directive cannot prevent the anonymous use of open networks such as the Internet.

3.4.2. EID concept

[45] See consideration No. 14.

The Directive does not have any specific data protection provision. However, the Directive builds especially on the Directive 95/46 EC as a general legal basis. The EID concept has therefore – as far as the Directive on e-commerce is applicable – taken due regard to the principles and provisions of the Data Protection Directive.

4. Summary Conclusions for EID

4.1. General conclusions

1. The EID aims to build a universally recognized electronic ID token for identifying citizens in multiple use case scenarios. The EID will make it possible to pass the identity, once issued, from one legal entity into other existing infrastructures of applicationswhether in the public or the private sector. In addition the EID will use certification service providers, most probably in the different national legislations. This proposal takes into account different functionalities and builds on various processes. From that perspective it is justified to speak not of the EID but rather of the "EID concept".

2. It has to be noted, that in most cases the roles of the different sectors are clearly defined in their specific areas of national regulations and thus the legal requirements follow the specific national legislation and the existing national legal organisational framework; e.g. the various European Member States have national data protection legislation and a matching national organisation. Although the European Directive 95/46 EC aims for harmonisation in European data protection, the differences in the various national data protection laws might be significant, e.g. the use of codes of conducts are accepted in some Member States but not in others.. This leads to a more complex legal assessment.

3. The legal assessment becomes more complex if, in addition to the various national areas of regulation, other geographical areas like e.g. the US or Japan have to be included in the EID concept. The European Union clearly has the most regulated environment as regards data protection and electronic signatures. US regulation tends to be more pragmatic than EU regulation and hence more flexible. Other regions of the world do not reach the level of US/European regulations.

4. The European Union has an advanced regulatory framework as regards protection of personal data. The European Directive relating directly to data protection is the Directive 95/46/EC of the European Parliament and the Council of 24th October 1995 on the Protection of individuals with regard to the processing of personal data and on the free movement of such data. In addition to the Directive 95/46 EC the European Commission has adopted a Decision 2001/497/EC setting out standard contractual clauses ensuring adequate safeguards for personal data transferred from the EU to countries outside the Union.

5. From a data protection perspective, the Directive 95/46 EC has to be identified as the main reference regulation for the EID concept. In addition to that Directive the Decision of the Commission 01/497 EC on standard contractual clauses has to be closely linked to that perspective as this Decision ensures adequate safeguards for personal data transferred from the EU to countries outside the Union. As the EID concept will include electronic signatures based on PKI the data protection provisions in the Directive 99/93 EC on electronic signatures have to be taken into account as well.

6. The Directive on e-commerce does not have any specific data protection provision. However, the Directive builds especially on the Directive 95/46 EC as a general legal basis. The EID concept has therefore – as far as the Directive on e-commerce is applicable – taken due regard to the principles and provisions of the Data Protection Directive.

4.2. Conclusions as regards data protection and EID

1. The EID concept will lead to a processing of personal data by automatic means, whereby data are either processed on the EID card itself or will be closely linked to the automatic processing of personal data outside the EID card using various databases. In any case the EID card will be connected to the processing of personal data by automatic means.

2. Independent of the decision who is determining the purposes and means of the processing of personal data, it has to be noted for the EID concept, that independent of the establishment of the data controller within the European Union, the same level of data protection pursuant to the Directive has to be implemented by the member Sates. This principle is of some practical importance and has to be taken into account as regards organisational issues of the data contoller. If the data controller is one entity or organisation the national data protection laws have to be applied, where this data controller has its establishment. If the EID concept plans to have several distributed data controllers the concept has to take into account that several national implementations of the Directive have to be in place.

3. To issue the EID it will be necessary to collect, store and process personal data at various levels or steps: identification and registration of the card holder, provision of applications to the card holder and provision of services (content) to the card holder. The EID token may carry additional information or personal data on the card itself. Personal data will be either processed on the EID card itself or will be closely linked to the automatic processing of personal data outside the EID card using various databases.

4. Within the EID concept it has to be discussed whether the processing of personal data takes place on the card itself or outside the card; this may have some effect on the definition and accordingly on responsibility for the various data protection provisions which are imposed on the data controller. In this context it has to be discussed furthermore what roles the various parties within the EID concept will have from a data protection perspective.

5. The description of functionalities from a smart card point of view are not sufficient from a data protection point of view. The EID concept has to take into account that it is not possible to nominate one single data controller, but it has to recognize that several possible data controllers are at stake: the card issuer, the application provider and the content or the service provider. It is therefore recommended to include at least the “content or service provider” in any data protection provision within the EID concept. In addition to the above discussed roles of the “data subject” and the “data controller” the Directive 95/46 EC identifies the roles of the “processor”, the “third party” and the “recipient”. It is also recommended that these roles be added to the data protection provision within the EID concept.

7. Confidentiality of the personal data while processed and security of the processing itself are a “must” when protecting the personal data of a data subject. Using a smart card within data processing with its many technical options is a challenge for these principles and, at the same time, an opportunity to provide a technically viable solution for safeguarding confidentiality and security of the processing of personal data. The EID concept has to watch these two principles very carefully. Any threat of unwanted disclosure of personal data on the smart card or from a database will

question the reliability of the card itself and thus reduce acceptance of the technology by the data subject.

8. It is recommended that the EID concept should have one overall security concept which would implement in general terms the required security features and thus would contribute to a harmonized approach for the EID concept. The GIF model should cover this issue.

9. The “magna carta” of any data protection regulations are the rights of the data subject. These rights enable the data subject to have transparency on the processing of personal data, they enable the data subject to judge the purposes of any processing of his personal data, to view stored personal data and to reject unlawful processing. At the same time the correct execution of these rights puts the obligation on the data controller to inform the data subject of any processing step. This information is the basis for the trust relationship between the data subject and the data controller.

10. The necessary information to the data subject has to be provided either by the card issuer, the application provider and/or the content or service provider. Within the EID concept this situation could end in a multiple information exercise, which is possibly leading more to confusion by the data subject than to transparency. It would be desirable to concentrate the required information on one specific data controller, which could be the card issuer. As long as the intended processing of personal data is known, this “combined information” to the data subject is a reasonable way of handling the required information. Nevertheless this simplification will not relieve any other content or service provider who is added later on to the EID framework from his obligation regarding information.

11. The EID concept has to enable the execution of the rights to access, rectification, blocking, or deletion of personal data without any constraint and without excessive delay or expense. The use of the EID card for accessing this information online is more appropriate than a written procedure.

12. For cases where data is transferred to non-EU countries, the Directive includes, in Article 25 and Article 26, provisions to prevent the EU rules from being circumvented. The basic rule is that the data should only be transferred to a non-EU country if it will be adequately protected there, although a practical system of exemptions and special conditions also applies (such as for data where the subject has given consent or which is necessary for performance of a contract with the person concerned, to defend legal claims or to protect vital interests (e.g. health) of the person concerned).

13. An “EID Model Contract on transfer of personal data to non-EU countries” could help to ensure the acceptance of the transfer of data to non-EU countries. The EID concept may establish safeguards that make them less dependent on the good will of the legislators of a given country. Even in the best case scenario, a number of non-EU countries are likely to fall short of an "adequate" level of protection, and individuals may be reluctant to give their consent to the transfer to such countries of their personal data. In addition this “EID Model Contract” would speed up the process with multiple private companies and/or public agencies. This standard “EID Model Contract” could be an integral or an annexed part of the Code of Conduct.

14. The certification-service provider within the EID concept has to follow the specific data protection regulation pursuant to Article 8 of the Directive on electronic signatures by focusing the personal data which may be collected and processed by the certification-service provider strictly to the purposes of issuing and maintaining the

certificate. By this the personal data processed will be very limited, unless the data subject explicitly consents to processing for other purposes. It is recommended that this specific provision be taken into account in the Code of Conduct.

15. Any processing of personal data within the EID concept must be lawful and fair to the data subjects. In particular data within the EID concept must be adequate, relevant and not excessive in relation to the purposes for which they are processed; the purposes must be explicit and legitimate and must be determined at the time of collection of the data; the purposes of processing further to collection shall not be incompatible with the purposes as they were originally specified.

16. It is recommended that the major principles on data quality be mentioned explicitly in the Code of Conduct. It is the responsibility of each data controller to safeguard the data quality. Moreover the issue of identification of the data subject has to be addressed in the Code of Conduct.

17. It is mandatory that the collection, the storage and any other processing of personal data are in line with the requirements of the Directive 95/46 EC. In addition to the principles for data quality in Article 6 the Directive uses accepted principles to provide legitimacy to data processing, especially the informed consent of the Data subject. It is recommended that the different usage scenarios, the sectors affected and the personal data necessary for processing are discussed in more detail as soon as usage scenarios are defined.

18. The EID concept may lead to some kind of an identification number, e.g. by using a certificate, a pseudonym or any other identifier. This universal number would have to face severe fears of the data subjects as it would possibly allow the accumulation of personal data around the unique identifier, from various databases and eventually end in a personal profile. The Directive addresses this issue in Article 8 paragraph 7, but leaves the question up to the Member States to determine the conditions under which a national identification number or any other identifier of general application may be processed.

4.3. Conclusions as regards next steps

1. The Code of Conduct for EID related data protection is a valuable and accepted contribution from the Directive's point of view. In addition, it would help to overcome to a certain extent the need to match the EID concept not only to the Directive but also to the implementation of the data protection legislation in Member States. The Code of Conduct will be "soft law" and it has to be matched against all implementations by the Member State or the Member States. It does not replace national legislation, but it would support initiating such kind of legislation in the Member States.

2. Decisions on Codes of Conduct on the Community level will have to take into account the data protection regulations of the Member States, i.e. the Working Party will have to match the proposed Code of Conduct to each Member State where it is intended it will be applied. The EU Commission is authorised to publish the Code of Conduct, as soon as the Working Party has approved the Code of Conduct.

3. In relation to the "Rules of conduct for privacy and card integrity" it is recommended the rules be matched to the national data protection rules pursuant to the Directive

and that these rules are proposed to the Working Party according Article 29 by an appropriate industry association.

4. An “EID Model Contract on transfer of personal data to non-EU countries” could help to ensure the acceptance of the transfer of data to non-EU countries. This standard “EID Model Contract” could be an integral or an annexed part of the Code of Conduct.

Annex 1: Overview on national data protection legislation, February 2002

Reference: http://europa.eu.int/comm/internal_market/en/dataprot/law/impl.htm

Member State	**Status of legislative procedure**	
Belgium	1) Consolidated text of the Belgian law of December 8, 1992 on Privacy Protection in relation to the Processing of Personal Data 2) modified by the implementation law of December 11, 1998 (O.J. 3.2.1999) English version: http://www.law.kuleuven.ac.be/icri/papers/legislation/privacy/engels/ 3) Secondary legislation adopted on 13th February 2001 and published in the Official Journal the 13th of March 2001. 4) Entry into force the 1st September 2001 (exception for information when the data were not collected from the data subject then 3 years more).	
Denmark	1) The Act on Processing of Personal Data (Act No. 429) of 31 May 2000 English version: http://www.datatilsynet.dk/include/show.article.asp?art_id=443&sub_url=/lovgivning/indhold.asp&nodate=1 2) Entry into force: 01.07.2000.	
Germany	1) The Federal Data Protection Act (Bundesdatenschutzgesetz) was adopted 18 May 2001, published in the Bundesgesetzblatt I Nr. 23/2001, page 904 on 22 May German version : http://www.bfd.bund.de/information/bdsg_hinweis.html English version : The Federal Data Protection Act will covers Federal public authorities as well as private sector. 2) Entry into force: 23 May 2001. Six Länder (Brandenburg, Baden-Württemberg, Bayern, Hessen. Nordrhein-Westfalen, Schleswig-Holstein) adopted new DPLs persuant to the Directive. These acts apply to the public sector of the respective "Länder". Brandenburg: Gesetz zum Schutz personenbezogener Daten im Land Brandenburg (Brandenburgisches Datenschutzgesetz - bgDSG) in der Fassung der Bekanntmachung vom 9. März 1999: http://www.brandenburg.de/land/lfdbbg/gesetze/bbgdsg.htm Baden-Württemberg: Gesetz zum Schutz personenbezogener Daten (Landesdatenschutzgesetz - LDSG) vom 27. Mai 1991, zuletzt geändert durch Artikel 1 des Gesetzes zur Änderung des Landesdatenschutz-gesetzes und anderer Gesetze vom 23. Mai 2000: http://www.baden-wuerttemberg.datenschutz.de/ldsg/ldsg-inh.html Bayern: Bayerisches Datenschutzgesetz (BayDSG) vom 23. Juli 1993, zuletzt geandert durch Gesetz zur Anderung des Bayerischen Datenschutzgesetzes vom 25.10.2000 (Inkrafttreten zum 01.01.2001): http://www.datenschutz-bayern.de/recht/baydsg_n.pdf Nordrhein-Westfalen: Gesetz zum schutz personenbezogener Daten (Datenschutzgesetz Nordrhein-Westfalen-DSG NRW-) in der Fassung der Bekanntmachung vom 9. Juni 2000: http://www.lfd.nrw.de/fachbereich/fach_3_1.html Hessen: Hessisches Datenschutzgesetz (HDSG) in der Fassung vom 7. Januar 1999	

	Precise page (one of the frames): http://www.datenschutz.hessen.de/hdsg99/Inhalt.htm Schleswig-Holstein : Schleswig-Holsteinisches Gesetz zum Schutz personenbezogener Informationen vom 9. Februar 2000 http://www.datenschutzzentrum.de/material/recht/ldsg-neu/ldsg-neu.htm Sachsen-Anhalt : Gesetz zum Schutz personenbezogener Daten der Bürger (DSG-LSA) http://www.datenschutz.sachsen-anhalt.de/dsg-lsa/inhalt.htm	
Spain	1) Ley Orgánica 15/1999, de 13 de diciembre de Protección de Datos de Carácter Personal. ("B.O.E." núm. 298, de 14 de diciembre de 1999). Original version: https://www.agenciaprotecciondatos.org/datd1.htm English version: 23750 ORGANIC LAW 15/1999 of 13 December on the Protection of Personal Data. 2) Entry into force: 14.01.2000.	
France	1) Law 78-17 of 6 January 1978 2) draft implementation law of July 2001 http://www.justice.gouv.fr/actua/loicnild.htm	
Greece	1) Implementation Law 2472 on the Protection of individuals with regard to the processing of personal data Original version English version 2) Entry into force: 10 4.1997	
Italy	1) Protection of individuals and other subjects with regard to the processing of personal data Act no. 675 of 31.12.1996. English version: http://www.dataprotection.org/garante/prewiew/1,1724,448,00.html?sezione=120&LANG=2 2) Entry into force: 8.5.1997 3) Additional legal acts previewed by Act no. 676 of 31.12.1996 (in particular, the Legislative Decrees no. 123 of 09.05.97, no. 255 of 28.07.97, no. 135 of 08.05.98, no. 171 of 13.05.98, no. 389 of 06.11.98, no. 51 of 26.02.99, no. 135 of 11.05.99, no. 281 and no. 282 of 30.07.99 ; the Presidentials decrees No. 501 of 31.03.98, No. 318 of 28.07.99)	
Ireland*	Draft bill to be approved by the Government and submitted to Parliament	
Luxembourg*	A new DPL was submitted to Parliament beginning October 2000.	
The Netherlands	1) DPL approved by the Senate on 06.07.2000 (O.J. 302/2000). Original and English version: Personal Data Protection Act (Wet bescherming persoonsgegevens), Act of 6 July 2000 2) Entry into force on 1 September 2001. 3) Secondary legislation adopted	
Austria	1) Bundesgesetz über den Schutz personenbezogener Daten (Datenschutzgesetz 2000 . DSG-2000) vom 17.08.1999 original version: http://www.bka.gv.at/datenschutz/dsg2000d.pdf English version: HTML version: http://www.bka.gv.at/datenschutz/dsg2000e.htm PDF version: http://www.bka.gv.at/datenschutz/dsg2000e.pdf	

	2) Entry into force: 1.01.2000. 3) Adopted ordinances: • Verordnung des Bundeskanzlers über den angemessenen Datenschutz in Drittstaaten (Datenschutzangemessenheits- Verordnung - DSAV), Federal Law Gazette II Nr. 521/1999, about countries with adequate DP legislation (Switzerland and Hungary); • Verordnung des Bundeskanzlers über das bei der Datenschutzkommission eingerichtete Datenverarbeitungsregister (Datenverarbeitungsregister-Verordnung 2000 - DVRV), Federal Law Gazette II Nr. 520/1999, about the registration procedure; • Verordnung des Bundeskanzlers über Standard- und Musteranwendungen nach dem Datenschutzgesetz 2000 (Standard- und Muster-Verordnung 2000 - StMV), Federal Law Gazette II Nr. 201/2000, about exceptions from notification.	
Portugal	1) Directive implemented by Law 67/98 of 26.10.1998. 'Lei da protecçao de dados pessoais' English version: http://www.cnpd.pt/Leis/lei_6798en.htm 2) Entry into force: 27.10.1998	
Sweden	1) Directive implemented by SFS 1998:204 of 29.4.98 and regulation SFS 1998:1191 of 03.09.98 English version: http://www.datainspektionen.se/in_english/default.asp?content=/in_english/legislation/data.shtml 2) Entry into force: 24.10.1998.	
Finland	1) The Finnish Personal Data Act (523/1999) was given on 22.4.1999 English version: http://www.tietosuoja.fi/uploads/hopxtvf.HTM 2) Entry into force: 01.06.1999.	
United Kingdom	1) Data Protection Act 1998 http://www.hmso.gov.uk/acts/acts1998/19980029.htm 2) Passed: 16.07.1998 3) Subordinate legislation passed on 17.02.2000. http://www.lcd.gov.uk/foi/foidpunit.htm 4) Entry into force: 01.03. 2000.	

Annex 2: Overview on EU directives and decisions on data protection and privacy

1. The European Directive relating directly to the data protection is the Directive 95/46 EC of the European Parliament and the Council of 24th October 1995 on the Protection of indivduals with regard to the processing of personal data and on the free movement of such data.[46]
2. The European Commission has adopted a Decision 01/497 EC setting out standard contractual clauses ensuring adequate safeguards for personal data transferred from the EU to countries outside the Union.[47]
3. Directive 97/66 EC of the European Parliament and of the Council of 15th December 1997 concerning the processing of personal data and the protection of privacy in the telecommunications sector.[48]
4. The European Parliament and the Council of Ministers have adopted the Regulation on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data, Directive 01/45 EC.[49]
5. The European Parliament and the Council of Ministers have adopted the Directive 99/93 EC of 13th December 1999 on a Community Framework for Electronic Signatures.[50]
6. The European Parliament and the Council of Ministers have adopted the Directive on a Legal Framework for Electronic Commerce 00/31 EC, which was adopted on 8th June 2000.[51]

[46] Official Journal L 281, 23/11/1995 P. 0031 - 0050

[47] Official Journal L 181, 4/7/2001 P. 0019 - 0031

[48] Official Journal L L 024 , 30/01/1998 P. 0001 - 0008

[49] Official Journal L 008, 12/01/2001, P. 0001 - 0022

[50] Official Journal L 13, 19.1.2000, P. 0012 - 0020

[51] Official Journal L 178, 17/07/2000, P. 0001 - 0016