XV CONGRESO NACIONAL DE ÉTICA DE LA ECONOMÍA Y DE LAS ORGANIZACIONES
EL BUEN GOBIERNO DE LAS ORGANIZACIONES
IESE BUSINESS SCHOOL
BARCELONA, 8 Y 9 DE JUNIO DE 2007

CORPORATIVE SOCIAL RESPONSIBILITY VIRTUAL ENVIRONMENTS

Manel Medina, Francisco de Quinto

KEYWORDS
Best practices, code of conduct, corporate social responsibility, digital identity, ethical issues.

TABLE OF CONTENTS

1. Introduction

All the indicators aim at the unstoppable and progressive digitization of relational processes among individuals and corporations to all levels: Business, social relations, teaching, health, regional government's bodies etc…

All this configures the so-called virtual surroundings brought of the convergence of information systems and telecommunications networks which has involved into the digitization of information paradigm.

Nowadays to think about some develop is difficult.

The objective of this paper is the search of concepts and tools that will make possible the development of stock CSR at surroundings digitized by means of the strengthening of confidence of the users starting from establishing the ethical necessaries of one´ s own of good corporate government, also in the companie´s virtual relations.

Therefore we propose the implantations in the systems ICT (Information Technologies and of the Telecommunications) of so-called ethical codes, best practices since they come from these various manners named.

As example we propose the contents of concrete model of ethical code. Not surprisingly, ethical code is not held in the void in spite of the virtuality of his area of responsibility, its operativeness is held in three concepts that integrate equally technological, legal and organizational components: Identity balanced, identity digital management and Circle of trust.

Ethics concerns questions about good and bad- the good life. Ethics is employed in order to perform better, to assure that the choices made are conducive to what is perceived as good for all parties involved- directly or indirectly. The actions of an enterprise have an impact on people, and ethics can assist when taking a responsibility for ones owns actions.

The involvement of governmental and other bodies in encouraging and facilitating the development of codes of practice and other self-regulatory mechanisms removes the spontaneity of self-regulation, and raises the question of whether industry organisations or individual firms have the motivation to pursue self-regulation in the long term, when neither regulatory oversight nor financial support for self-regulation are in place.

2. OPERATIVENESS

2.1 Identity balanced

Identity describes the distinction between an individual and a person, which can only be determined from the perspective of the person. The role then denominates the interrelation between activation of situation dependent identity properties and the corresponding form of the transmitting action.

The decision about a point in time for activation of a personal attribute, the combination of attributes in past and present and the respective profile of attributes are individually unique.

Together with the social constraint of identity profiles the individual aspect of a human's identity, which integrates all of these aspects, becomes visible for the first time.

Identity is communicable, as long as it is possible to name it. Therefore, this form of identity is also technically-operationally accessible.

Citizens have the right to be in charge of their privacy and personal data when using online services. On the Internet, privacy is a major concern for users, who are entitled to know and control what personal information will be shared with whom and want an assurance that information can be exchanged without third parties seeing it. Users of web-services want to be sure that the personal information they share will not be shared with anyone else without their permission.

The ability to maintain privacy and avoid unauthorized use of identity data are building blocks of trust, a prerequisite for the wide use of advanced information and e-business services. Misuse or inadequate protection of personal information can result in identity theft, financial fraud or other problems.

Systems that enable user control over privacy and identity data empower individuals to control their private sphere and manage their digital identities securely. This is crucial for the continued take-up of information and communication technologies, particularly in view of the emergence of more and more personalised services.

A Digital Identity is the representation of a human identity that is used in a distributed network interaction with other machines or people. The purpose of the Digital Identity is to restore the ease and security human transactions once had, when we all knew each other and did business face-to-face, to a machine environment where we are often meeting each other for the first time as we enter into transactions over vast distances.

In this simplest Digital Identity the user name is the identity while the password is said to be the authentication credential. This simple Digital Identity is encountered in a logon sequence, and calling it a Digital Identity may seem a bit much until you realize its purpose is to identify you to the system you are logging into.

As computerized systems become more networked and distributed, the Digital Identity must become more robust to make complex distributed user interactions easy while achieving the required control and security for the Digital Identity's information. Ultimately Digital Identity will become as complex and flexible in use as a real-world human identity.

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, may it be in the private sector, may it be in the public sector. To issue the ID token it will be necessary to collect, store and process personal data.

2.2 Digital identity management

In general we can distinguish between centralised identity and federated identity (and centralised and federated identity management):

Centralised identity means that users and providers enrol with a central IMS provider which issues unique (global) identifiers. The central IMS provider acts like a single gateway for the user's management of identities, e.g., in a single sign-on scenario the authentication of a user is performed by the central IMS provider.

Because of the single point of control the system is easier to maintain, it means less effort in user support, and it is cheaper. Disadvantages are possible breaches of security and privacy requirements, because the systems concentrate personal data of the users, which enables the provider itself and possibly other parties to monitor the users' behaviour.

The centralised concept puts big responsibilities on the providers, which should guarantee a high level of security and privacy.

Federated identities do not work with a single IMS provider. This category comprises both solutions with multiple IMS providers and implementations of user-side identity administration. As there is not one unique global identifier and no concentration of personal data outside the user's scope, users have (more) control over what personal data they share with whom.

The different service providers have control over user profiles, as far as they get to know them. For interoperation, standards of protocols and interfaces are required, (such as in Liberty Alliance). The lack of centralised control may lead to inconsistencies of data. Federated identity management puts bigger responsibilities on the user and can mean more effort in user support.

2.3 Circles of trust

A Circle of Trust (CoT) is defined by (Liberty Alliance) as a federation of service providers and identity providers that have business relationships based on Liberty architecture and operational agreements and with whom users can transact business in a secure and apparently seamless environment.

As federated communities create inter-dependencies and, consequently, the need for trust between participants, the CoT is viewed by the Liberty Alliance as an essential component of establishing a system of federated identity based on Liberty specifications.

The CoT therefore creates a trusted framework for both the participating service providers and identity providers but, perhaps most importantly, *the consumers, employees or end users whose identity is often the subject of federation.*

3. WHY A CODE OF CONDUCT

Because law and technology are two concepts that when integrated unties a difficult dialectic principally because the information and communication technologies (ICT) are characterized by their no spatial reference (disorientation; nowhere and anywhere) and on the contrary law is always necessary referred to specific territory because its essence is derived from a concept of sovereignty. As an example we give an appointment of the document Privacy and Security best practices by Liberty Alliance

"In addition to existing privacy laws, several organizations have set forth fair information practices governing the use and disclosure of personal information. These organizations include, among others, the Online Privacy alliance ("OPA"), the Organization for Economic Co-operation and Development ("OECD"), the Centre for Democracy and Technology ("CDT"), the Networked Advertising Initiative ("NAI"), Health Internet Ethics ("Hi-Ethics"), and the Global Business Dialogue on electronic commerce ("GBDe")"

"There are no universal standards among these organizations as to what fair information practices entail. The differences seen in these fair information practices are partially attributable to geography, and partially attributable to the sector to which the fair information practices apply."

"…there is a wide range of fair information practices that have been promoted around the world. In an effort to promote "best practices," Liberty recommends that an implementing company comply with all relevant law. In the absence of laws, an implementing company should follow the most appropriate fair information practise applicable to the jurisdiction and industry sector in which the company intends to do business or offer products or services. When applicable, an entity should not request or provide more information than is necessary for the interaction".

In order to respect self-determination it would be necessary to include information on:

- Which personal data is stored, for how long it is stored
- Which public authorities have a right to access the data, for which reasons and for how long
- Information on how one may delete personal data
- Options deleting or changing sensitive personal data

In order to respect for self-determination require confidentiality:

- Direct marketing is not employed without informed consent
- Personal data are not given to third parties and/or used in ways not describes in a contract.

Finally self determination is enhanced by multiple options of consent:

- Offer an active consent
- Provide appropriate and understandable information in a short form
- If practically feasible, provide the user an option to active consent in every single use or in a bulk.

4. THE ETHICAL MANAGEMENT GROUP

As LINUS, Kjersti Lunde, "Fidelity ethics report", July 2006 introduce in his ethics code of conduct, an ethical management group would as well necessary in order to complement an ethical code:

- The members should be representing various areas of the project, such as security, marketing, SP´s and other relevant domains.
- The members have a special responsibility in informing the Data Protection Official on factual problems and challenges met in the different parts of the network, advice, on practical options and secure follow-up of decision in the line
- The responsibility of the members is to secure flow of information on other relevant news and issues of importance to the management of the ethical policy and define action on them
- The group should be headed by the Data Protection Official which responsibilities are:
- The overall management of the ethical issues
- Formulation of an ethical policy describing all responsibilities and actions taken and planned, under the management of the Data Protection Official
- Formulation of an Ethic Code of Conduct describing in particular SPs responsibilities to protect the user´s interest
- Assure survey and update on security issues and initiative proactive action on them.
- At least reporting annually on ethical challenges, issues and activities, including how the requirements of an ethical character in EU regulation of the area and how the ethical principles are respected in practice for the user are complied.

5. PROGRAMME OF INFORMATION, EDUCATION AND AWARENESS

Following LINUS, Kjersti Lunde, "Fidelity ethics report", July 2006, giving the instruction for a programme of information, education and awareness:

- Creating a website for external communication with information in a non-technical and non-specialist language.
- As appropriate employ other means of communication.
- Promote awareness among users and SPs on ethical issues in relation to telecom services, including providing information and links to existing international law, regulation and guidelines, EU and national data protection authorities and other relevant information.
- Inform users on Privacy Enhancing Technologies and advice on how they best protect themselves both by wise and cautious action when using telecom services and inform about the appropriate technical security installations in user en
- Information on what kind of authorities may have access to personal data under which circumstances

6. BENEFITS

To help all the subjects involved to accomplish legal requirements.

To reinforce respect and human rights exercising existing international law as the European Convention on Human Rights and the European convention on the Protection of Individuals with regard to Processing of Personal Data that determine what are the basic human rights, which are relevant and which must be respected and protected.

The human rights must be interpreted in relation to the factual processes involve in. These rights are highly esteemed in democratic European culture i.e. Most are highly esteemed in democratic European culture.

Making a contribution in order to provide trust to the end users because a code of conduct reflects public attitudes and knowledge of security and privacy issues related to telecommunications services.

To what has been freely accepted benefits are derived and that is what happens with all of the Code of Conducts best practices and also what happens with Fidelity Code of conduct because there are no mandatory rules.

7. APPENDIX

A) Principles of a code of conduct:

Organizations must comply with the principles of this code of conduct. The principles require the following:

1. Identity digital management (IDM)

The connection between the components of the circle/s of trust is made through telecommunications infrastructures and the communication between components and identification of users involves electronic signature that provides a permanent and a strong authentication to the user.

Identity Digital Management allows that in each of the possible scenarios it could be developed a profile attribute of the user with independence of its own identification level.

2. End user's digital rights.

End users have the right to have relations with all the parties involved (subjects) integrated in CoTs in order to ask for information, make consultations, formalize requests and contracts, make payments and do any kind of transactions.(General principle)

Users have the right to access all the services and social benefits through its selection channel between those that could be at any moment and which finality is accessible. (Accessibility principle)

Users have the right of not provide any information or data that previously has been obtained by the suppliers of the CoT who will have that information when previously explicit consent has been asked. (Economy principle)

Users have the right to know at any moment and through electronic media, the state of the processes in which are involved also to have an electronic copy of the documents in which those processes are integrated. (Information principle)

Users have the right of utilizing any electronic certificate that accomplishes the European Directive requirements about electronic signature (Directive 19999/93/EC of the European Parliament and of the Council of 13 December 1999) and also to use it in order to manage its own IDM according to its criteria and needs. (Management identity principle)

Users have the right of obtain a security and confidentiality guarantee of its personal data which are contained in files, systems and applications which integrates CoTs according to the correspondent Communitarian Directives (Directive 95/46/EC and Directive 2002/58/EC) (Privacy principle)

Users have the right of having a good time with the legal electronic contents, accessible, transparent and comprehensible with quality. (Quality principle)

Users have the right of have the information, formation and help for the utilization of the contents from CoTs. (Sustainability principle)

3. Information, education and awareness

These principles involve the creation of a website for external communication within formation in a non-technical and non-specialist language as appropriate employ other means of communication.

To promote awareness among users and SPs on ethic issues in relation to telecom services including providing information and links to existing international law, regulation

and guidelines; EU and national data protection authorities and other relevant information as e.g. EU initiatives, EU Barometers Surveys, etc.

To inform users timely on security challenges and action taken by Fidelity, handle complaint from user and take the appropriate action, including e.g. warnings and exclusion of SPs if they do not comply with the Ethical Code of Conduct.

To inform user on Privacy Enhancing Technologies and advice on how they best protect themselves both by wise and cautions action when using telecom services (e.g. inform about pharming, phishing and other relevant malware), and inform about the appropriate technical security installations in user end.

To inform on what kind of authorities may have access to personal data under which circumstances.

4. Notice

In order to federate accounts, enjoy the convenience of single-sing-on, facilitate transactions to which principals are a party or to enable the exchange of attributes concerning to them it will be necessary to collect personal data so there are e-commerce activities in some scenarios.

Disclaimers has to be used in order to clearly define authorized operations involving user attributes and legal notices when asking for consent must inform the user about purpose, processing, distribution, conservation of data, protection of data, the warrantee of the accomplishment of right of access /modification / objection / cancellation, rectification that will be accessible to the user in a visible form providing the mechanisms to communicate the requests.

5. Choice

Components involved in data transfer will use personally identifiable information for the purpose or the purposes about which the principal has consented or legal ordered attending to the type of consent that is required according to the type of data that will be have to be transferred.

When countries involved in data transfer belong to the EU member states it will be necessary to notify the Control Authority before transfer the data but if third countries that not belong to the EU member States and that are not considered by specific agreements, security measures can not be assured and privacy rights can be in danger. Because of this situation it will be necessary the explicit consent from the user to transfer the data to third countries, except if the transfer is necessary for the performance of a contract, pre contractual measures, or for the conclusion or performance of a contract concluded.

The transfer takes place on standard contractual terms approved by European commission and prior authorization of the relevant Member States privacy authority has to be given before transfer takes place.

No data cession, it is guaranteed not to transfer the data obtained from a minor to third parties.

6. Onward Transfer

The effect of the adoption of a Commission decision based on Article 25.6 of the Directive is that personal data can flow from the 25 EU member states and three EEA member countries (Norway, Liechtenstein and Iceland) to that third country without any further safeguard being necessary. The Commission has so far recognized Switzerland, Canada, Argentina, Guernsey, Isle of Man, the US Department of Commerce's Safe Harbor Privacy Principles, and the transfer of Air Passenger Name Record to the United States' Bureau of Customs and Border Protection as providing adequate protection.

An exception from the adequacy requirement for trans-border data flows out of the EU is where the transfer takes place on standard contractual terms.

Standard clauses in bilateral contractual arrangements establish that all the entities that participate in this Circle of Trust fully adhere with no rejections to this Code of Privacy and Security Best Practices from Liberty Alliance that regulates the Circle of Trust and declines any liability related to usage and conduct of the users out of the scope of the Code of Conduct.

7. Access

In order to guarantee the integrity of the data the controller and the processor (components) noticing the existence of the right to access, must guarantee every data subject right to obtain confirmation of the data related to principals, the purposes of the processing, the categories of data concerned and the recipients or categories of recipients to whom the data are disclosed and its consequent communication in an intelligible form.

Control of the user’s age in case of personal data request to the minor, the user must be asked about his/her age, to grant that data will not be requested children younger than 14 years-old

8. Accessibility

Electronic and computer media and also applications and programmes used for the Fidelity Project architecture must be used on a ample manner, not discriminatory being to disposition of all the subjects that participate or integrate the CoTs and in special must guarantee the easy access to the final users through more compatible and generalized technologies.

9. Security

All the entities that participate in the circle of trust must take reasonable steps in order to protect and provide an adequate level of security for Personally Identifiable Information, according to the Type of Data in order to protect 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.

10. Data integrity

In order to ensure legitimacy of the process consent must be given freely, informed of the purposes for which consent is sought and specific and of the duration of described by the service provider to the user or subscriber.

Commitment of destruction of data obtained from a minor, it must be granted that the data not needed to be kept by a legal imperative will be destroy once the good or service has been provided. The electronic communication systems must provide a system of authentication, identity protection and message protection mechanisms.

Encryption of messages will be necessary in the Service Level Agreement through the adequate parameters of the Artefact Profile when private data relative to religion, ideology, trade unions membership, sexual life, race and health will have to be authenticated when a user have express its explicit consent.

Store information or to gain access to information stored in the terminal equipment of a subscriber or user, is only allowed on condition that the subscriber or user concerned is provided with clear and comprehensive information.

11. No use of illegal contents

Components will not use illegal contents that are prohibited in a general manner to the society that constitute crime according to the national and international criminal legislation as contents related to infantile pornography and to infantile prostitution, including the infantile sex tourism, too. Contents that causes discrimination, violence and hate by racist and religious reasons, discrimination, violence and hate by other reasons such as the ones referred to ideology, sex, nationality, sexual orientation, illness or disease. Contents related to activities against public health in particular toxic drugs or narcotics and contents that can induce suicide. Contents that attempt against the rights of the personality: Honour, privacy and self image, also contents relative to explosives, substances and items that may cause damage. Contents that induce to the abandonment of domicile and illicit advertising

12. Respect of Industrial and Intellectual property rights

Components must respect the material protected by intellectual or industrial property rights belonging to third parties, it is compulsory to previously obtain from the holders of theses rights the authorisation necessary for the use that is made of it or plan to make of it.

13. Communications with consent

The commercial communication can be sent after receiving the express request or consent of the addressee

Procedures by which persons receiving services can at any time rescind the consent that they made must be simple and free and with clear information about how to do so.

Including information, advertising must be clearly distinguishable from other contents

14. Protection of minors.

Components will protect minors from the injurious contents that are those that being able to be accessible for the adults are susceptible to affect the physic or mental development of the minor which amongst other are the following:

Content related to sex, out of an artistic, medical or scientific range, with free violence or that may induce to aggressive conducts, that promote a discriminatory treatment, as long as they are not criminal, that may promote alimentation disorder, beauty and easy success stereotypes, consumption of tobacco, alcohol, chance, games, medicines or medical or esthetical treatments, fear or superstition and contents of terror that may cause physic alterations, contents that may endanger the minor or that may be perceived as annoying or uncomfortable, that use or promote the use of an inadequate language of the minor, advertising contents related to the minor as consumer.

The age of the minor must be verified in order to enable his/her capability to hire.

15. Enforcement

Procedures for verifying that the commitments companies make to adhere to code of conduct principles are implemented in order to decide if an actor continues taking benefits of in the circle of trust

B) Example of a code of Best Practices in Federated Identity Scenarios:

I. Code of Privacy and Security:

1 Personal data must be processed fairly and lawfully (Art., 6, a EU DPD)

Personal data must be collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes (Art 6.b EU DPD),

3 Personal data must be adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed (Art. 6. c EU DPD)

4, Personal data must be 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 (Art 6,d EU DPD),

5. Personal data must be kept in a form which allows 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 (Art... 6.e EU DPD),

6. Personal data must be retained for a period no less than 6 months and no longer than 2 years (Art 6 EU 2006/24/EC).

7. Personal data must be processed only if the data subject has unambiguously given bis consent (Art 7.a EU DPD) or„,

8. 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 (Art 7..b EU DPD),

9. **The processing of special categories of data.** The processing 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 is prohibited by Member States (Art 8A EU DPD).

10. Paragraph 9 shall not apply where the data subject has given his explicit consent to the processing of those data (Art 8.2.a EU DPD).

11 Paragraph 9 shall not apply where 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 (Art 8.2.b EU DPD).

12. Processing of data relating to offences, criminal convictions or security measures and the data relating to administrative sanctions or judgements in civil cases may be carried out only under the control of official authority (Art 8,3 EU DPD).

13 **Information in cases of collection of data from the data subject.** In order to guarantee fair processing in respect of the data subject, the controller or his representative must provide a data subject from whorn data relating to him are collected with at least the following information, except where he already has it:

(a) the identity of the controller and of his representative, if any;

(b) the purposes of the processing for which the data are intended;

(e) any further information such as: the recipients or categories of recipients of the data, whether replies to the questions are obligatory or voluntary, as well as the possible consequences of failure to reply, the existence of the right of access to and the right to rectify the data concerning him (Art 10 EU DPD),

14. Information where the data have not been obtained from the data subject. The controller must communicate the concerned the same cases explained in paragraph 13 no latter than the first communication (Art. 11 EU DPD).

15, Right of access. Controller and processor shall guarantee every data subject right to obtain

(a) without constraint at reasonable intervals and without excessive delay or expense:

- o 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,

- o communication to him in an intelligible form of the data undergoing processing and of any available information as to their source (Art. 12 a EU DPD).

16. **Right of rectification.** As appropriate the rectification, erasure or blocking of data the processing of which does not comply with the provisions of' the EU DPD, in particular because of the incomplete or inaccurate nature of the data (Art, 12.b EU DPD).

17 **The data subject's right to object.** Controller and processor shall grant the data subject the right to object at any time on compelling legitimate grounds relating to his particular situation to the processing of data relating to him, save where otherwise provided by national Where there is a justified objection, the processing instigated by the controller may no longer involve those data. (Art 14.a EU DPD),

18. **Automated individual decisions.** Controller and processor shall grant the right to every person not to be subject to a decision which produces legal effects concerning him or significantly affects him and which is based solely on automated processing of data intended to evaluate certain personal aspects relating to him, such as bis performance at work, creditworthiness, reliability, conduct, etc, except if that decision is taken in the course of the entering into or performance of a contract or it is authorized by a law which also lays down measures to safeguard the data subject's legitimate interests (Art 15..1 and 15.2 EU DPD).
19. **Confidentiality of processing.** Any person acting under the authority of the controller or of the processor, including the processor himself, who has access to personal data must not process them except en instructions from the controller, unless he is required to do so by law (Art.. 16 EU DPD),
20. **Security Measures of processing.** 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 sutured of the data to be protected (Type of data) (Art 17.1 EU DPD).
21. **Necessity of a contract between controller and processor.** 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:

    1... the processor shall act only en instructions from the controller,

    2. The obligations set out in paragraph 1, as defined by the law of the Member State in which the processor is established, shall also be incumbent en the processor (Art 17.3 EU DPD)...
22. **Obligation to notify the supervisory authority.** The controller or his representative, if any, must notify the supervisory authority before carrying out any wholly or partly automatic processing operation. Except if this processing whose sale purpose is the keeping of a register which according to laws or regulations is intended to provide information to the public (Art 18.1 and 18, 3 EU DPD).
23. **Contents of notification.** It shall include at least:
    (a) the narre and address of the controller and of bis representative, if any;
    (b) the purpose or purposes of the processing;
    (c) a description of the category or categories of data subject and of the data or categories of data relating to them;
    (d) the recipients or categories of recipient to whom the data might be disclosed;
    (e) proposed transfers of data to third countries;
    (f) a general description allowing a preliminary assessment to be made of the appropriateness of the measures taken pursuant to paragraph 20 to ensure security of processing (Art. 19 EU DPD),
39. **Principles of the transfer to a third country.** Personal data which are undergoing processing or are intended for processing after transfer may take place only if, without prejudice to compliance with the national provisions adopted pursuant to the other provisions of this Directive, the third country in question ensures an adequate level of protection (Art 25. EU DPD).
40. **Derogations.** A transfer or a set of transfers of personal data to a third country which does not ensure an adequate level of protection may take place on condition

that:

(a) the data subject has given bis consent unambiguously to the proposed transfer; or

(b) the transfer is necessary for the performance of a contract between the data subject and the controller; or

(e) The transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the controller and a third party; or

(c) the transfer is necessary in order to protect the vital interests of the data subject. (Art...26 EU DPD).

II. Request of Personal Data to Minors

41. Control of the user's age in case of personal data request to the minors. **The** users must be asked about his/her age, to grant that data will not be requested children younger than 14 years-old.

42. Requested data quality from the minor The data requested to the minor must be adequate for the finality of the request. It is guaranteed that the data obtained would not be used to elaborate socioeconomic profiles

43. No data cession. It is guaranteed not to transfer the data obtained from a minor to third parties.

44. Commitment of destruction of data obtained from a minor. It must be granted that the data not needed to be kept by a legal imperative will be destroyed once the good or service has been provided.

III. Code of General Contents

30. 'Illegal contents. Illegal contents are those that are prohibited in a general manner to the society neither (no matter what the age of the addressee is nor the support), In particular, illegal contents are those that constitute crier according the national criminal legislation and the international instruments that are pan of the Spanish legislation, amongst other, the following:

a. Contents related to infantile pornography and to infantile prostitution, including the infantile sex tourism, too.

b Contents that causes discrimination, violence and bate by racist and religious reasons,

e. Contents that causes discrimination, violence and bate by other reasons, such as the ones referred to ideology, sex, nationality, sexual orientation, illness or disease.

d. Contents related to activities against public health, in particular toxic drugs or narcotics.

e. Contents that induce suicide.

f. Contents that attempt against the rights of the personality:

honour, privacy and self image,

g. Contents related to terrorist activities.

h. Contents related to explosives, substances and items that may cause damage.

i. Contents that induce to the abandonment of domicile.

Illicit advertising.

31. Industrial and Intellectual Property Rights. In the case of use of material protected by intellectual or industrial property rights belonging to third panties, it compulsory to previously obtain from the holders of these rights the authorisation necessary -for the use that you make of it or plan to make of it.

32. Consumer protection. In the use of e-commerce, the regulations on consumer protection in force in Spain must be respected.

33. **Communications with consent.** The commercial communications can be sent after receiving the express request or consent of the addressee.

34. Procedures by which persons receiving services can at any time rescind the consent that they node must be simple and free and with clear information about how to do so,

35. Including information. Advertising must be clearly distinguishable from other contents,

IV. Code of Contents to the Minors

36. Injurious content. Injurious contents are those that being able to be accessible for the adults are susceptible to affect the physic or mental development of the minors, amongst other, the following:

a... Contents related to sex, out of an artistic, medical or' scientific range.
b. Contents with free violent or that may induce to aggressive conducts.
c. Contents that promote a discriminatory treatment, as long as they are not criminal.
d. Contents that may promote alimentation disorders...
e. Contents that may promote beauty and easy success stereotypes...
Contents that may promote the consumption of tobacco, alcohol, chance garners, medicines or medical or esthetical treatments.
g. Contents that promote fear or superstition and contents of terror that may cause physic-psychic alterations.
h. Contents that may endanger the minor or that may be perceived as annoying or uncomfortable...
i. Contents that use or promote the use of an inadequate language for the minor.
j. Advertising contents related to the minor as consumer.

37. Electronic hiring. The age of the minor must be verified in order to enable his/her capability to hire.

8. GLOSSARY OF TERMS

A principal: Is an entity that can acquire a federated identity, that is capable of making decisions and to which authenticated actions are done on its behalf. It can be an individual user, a group of individuals, a corporation, other legal entities or a component of the Liberty architecture.

Federated identity architecture delivers the benefit of simplified sign-on to users by granting rapid access to resources to which they have permission, but it does not require the user's personal information to be stored centrally.

Network identity is the fusion of network security and authentication, user provisioning and customer management, single sing-on technologies and web services delivery.

Service Provider (SP) is an entity that provides services and/or goods to Principals. **It is also named controller and/or processor.**

Data subject: Individuals are the subject of the personal data but small business and partnerships in the case of that any of their individual members or partners can be identified, they may be treated as data subjects depending on the legal nature of the entity concerned.

Public electronic communications network provider: Transmission system

Public electronic communications services provider: Provide electronic communication networks, including telecommunications services and transmission services in networks used for broadcasting.

User: Uses or request an electronic communication can be also subscriber.

9. BIBLIOGRAPHY

ALVAREZ DE LOS RÍOS, José Luis: "Delitos informáticos". Ponencia en las Jornadas sobre Marco legal y Deontológico de la Informática. Mérida 17 de septiembre de 1997.

BAÓN RAMÍREZ, Rogelio: "Visión general de la informática en el nuevo Código Penal", en Ámbito jurídico de las tecnologías de la información, Cuadernos de Derecho Judicial, Escuela Judicial/Consejo General del Poder Judicial, Madrid, 1996, págs. 77 a 100.

BELLO JANEIRO, Domingo: "El derecho a la intimidad y a la privacidad y las administraciones públicas". Escola Galega de Administración Pública. 2001.

BERLEUR Jacques y BRUNNSTEINS Klaus. "Ethics and computing. Codes, spaces for discussion and law". White paper from the EIFEL. Discussion group. Future Internet

CAMPRUBÍ, Abel y varios autores: "Manual pràctic d´Internet a l´empresa. Vol I". COPCA. Barcelona 2001.

GOEMANS, Caroline y DUMORTIER, Joe. "Enforcement issues. Mandatory retention of traffic data in the EU: possible impact on privacy and on-line anonymity".

CARRETERO GUTIERREZ, Maria José (Dirigido por José Galindo Gómez). Libro Web sobre ética aplicada a la informática. Escuela técnica superior de Ingeniería Informática, Universidad de Málaga, 2006.

DE QUINTO ZUMÁRRAGA, Francisco. Sistemas de responsabilidad social en entornos empresariales. Un diseño desde la perspectiva de la complejidad. XI Conferencia anual de ética, economía y dirección. (EBEN España) Junio 2003.

DUMORTIER, Joe y GOEMANS, Caroline. Roadmap for advanced research in privacy and identity management. December 2002.

INDEPENDET CENTRE FOR PRIVACY PROTECTION (ICPP). "Identity Management Systems (IMS)". Identification and comparison study

DUMORITER, Joe "Information Society and Media. ICT for trust and security. Legal considerations with regard to privacy protection and identity management in the information society". European Commission.

ENGEL-FLECHSIG, Stefan "Study on legal issues in relation to the use of public ID (Electronic Identity)" Radicchio Ltd. UK, 15th October 2002

VARNEY, Christine Y HOGAN AND HARTSON. "Liberty Alliance Project. Deployment Guidelines for Policy Decision Makers". September 21, 2005.

VARNEY, Christine, Hogan and Hartson Liberty Alliance Project. Privacy and Security Best Practices. Novembre 12, 2003.