10593/02/EN
WP 73

Working Document on E-Government

Adopted on 8 May 2003

THE WORKING PARTY ON THE PROTECTION OF INDIVIDUALS WITH REGARD TO THE PROCESSING OF PERSONAL DATA

Set up by Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995[1],

Having regard to Articles 29 and 30 paragraphs 1 (a) and 3 of that Directive,

Having regard to its Rules of Procedure and in particular to Articles 12 and 14 thereof,

HAS ADOPTED THE PRESENT WORKING DOCUMENT:

INTRODUCTION

The development of e-government constitutes today in most of the Member States one of the priority axes of action within their administrative modernization policies. Such priority is also expressed at European level with the adoption by the European Council of Feira in June 2000 of the "action plan e-Europe 2002" which includes a chapter on "on-line administration".

Thus, at the moment we can observe the development of various types of e-government projects which consist in setting up and promoting the on-line supply of administrative procedures. It appears that in some of these projects complex data protection issues are involved which need careful consideration in order to ensure the success of e-government projects.

As examples one may mention the institution of a unique entry point to online administrative services, of unique identifiers or the implementation of interconnections of public databases.

This document aims at presenting the state of affairs of electronic government (e-government) and the protection of individuals regarding the processing of their personal data in the European Union. It is meant to contribute to the reflection on this topic. The document drafted by the French delegation constitutes a synthesis of the answers given by the data protection authorities represented in the Working Party to a questionnaire on these questions.

Upon consideration of the constant evolution of electronic administration services and of conclusions reached from experience made in this area, the Working Party might come back on these issues in the future, with a view to providing further guidance on the application of the rules of Directive 95/46/EC in this context.

---

[1] Official Journal no. L 281 of 23/11/1995, p. 31, available at: *http://europa.eu.int/comm/internal_market/en/dataprot/index.htm*31, available at: http://europa.eu.int/comm/internal_market/en/dataprot/index.htm

A. CONSULTATION AND INITIATIVES OF DATA PROTECTION AUTHORITIES RELATIVE TO E-GOVERNMENT ISSUES

All European Data Protection Authorities have somehow expressed their views on electronic government issues.

1. In the large majority of the cases, Data Protection Authorities were officially consulted by public authorities. In general, this consultation is formally required for the administration to comply with the procedures laid down in national data protection law, on occasions when legislative or regulatory measures are taken by the administration that have implications on data protection, or at on the occasion of the implementation of particular online administrative procedures. In this respect, several Authorities have mentioned that this obligation of consultation of the Authority is not systematically respected by the authorities. The administration could also consult the Authority in a spontaneous way on matters of electronic government.

2. The Authorities could also give their opinion in public debates or on the occasion where reflections launched on the subject by public authorities. This was the case in France, where the CNIL was associated by government to the public discussion led on these questions and made its first elements of reflection public on the issue in its last annual report, or in the United Kingdom, where the Information Commissioner, which was not formally consulted by the public authorities, gave its opinion by commenting on various governmental proposals or by taking part to public consultations.

3. The opinion of Data Protection Authorities on E-government issues can also have resulted from the DPAs' own initiatives. In the Netherlands, for example, the Authority took the initiative to express its opinions on the subject without any specific occasion.

4. Finally, some Authorities can belong to working groups on specific projects of E-government (Finland, Netherlands, France, in particular) or have required to be informed of the evolution of specific projects (Portugal).

The consultations and initiatives of the Authorities could relate to the general framework of the development of the electronic government, or to specific issues.

The contributions of the various delegations show that the topics of the questions dealt by the Authorities are very diverse. It can first of all be an opinion bearing on overall projects, such as, in Spain, the establishment of an electronic identity card or the implementation of a general project of e-government promotion; in Sweden, the implementation of a "common policy" of the Swedish Bankers Association and the Post Office concerning the electronic identity card; in Italy, in addition to the emission of an electronic identity card, the implementation of a national project of establishment of a "unified network of public administration", i.e. an electronic network connecting all the administrative authorities of the country.

DPAs may also have intervened on the occasion of the implementation of specific online administrative procedures, such as, concerning personal taxation, the online income tax declaration and on line tax payment; concerning social security, the on line declaration and reimbursement of health costs (Spain, France), etc. In these cases DPAs particularly insist on the issue of data security.

Opinions were also given on the occasion of the introduction in national law of particular texts, such as the European Directive on electronic signatures (in particular in Finland, where the law of transposition will be in force at February 1, 2003, Denmark, where the DPA has given an opinion regarding draft legislation on the issue and Spain, where the DPA has released a report on draft legislation).

B. STATE OF DEVELOPMENT OF PUBLIC ONLINE ADMINISTRATIVE PROCEDURES

This question aimed at knowing, in each country, the level of development of online administrative procedures as well as the corresponding security level implemented, in accordance with the list of the 20 basic procedures that should be offered on line, in accordance with the action plan e-Europe established in view of the European Council of Feira (June 2000). Only 8 countries filled out the table.

With the exception of Belgium and Germany, all data protection authorities were consulted on the projects of online administrative procedures implemented in their country.

In general, DPAs' observations primarily related to security measures, and more specifically to measures of identification and authentication of users as well as of agents or professionals allowed to have access to applications of online administrative procedures. In the same way, the encryption of data during its transmission constitutes a security measure that is generally recommended as well as, to a lesser extent, encryption during the data storage and the implementation of data loggers and of logfiles (Portugal, Netherlands, France, Austria).

In addition, Data Protection Authorities also all agree that the development of the on-line administrative procedures must be accompanied by information measures for citizens, in particular on the rights which they are granted according to data protection legislations.

1. First of all, all the countries mentioned above offer to individuals the possibility to have recourse to an on-line procedure of income tax declaration, often associated, besides, to the possibility of on-line payment (6 countries) and of on line consultation of the person's file (6 countries also).

   In the same way, among the online administrative procedures offered to the companies, the service most frequently quoted relates to on-line tax declaration, concerning VAT (8 countries) or direct taxes (6 countries).

   The sector of public finance thus undoubtedly constitutes the privileged field of intervention of electronic government**.** It should be noted that the online administrative procedures offered in this field generally give rise to a higher level of security than other online administrative procedures, several countries indicating that they have resort to electronic signature systems (Finland, Spain,

France), or of data encryption (France, Portugal, Spain). In Austria access is secured by passwords only.

2. The administrative notification of change of address, insofar as this step constitutes a usual (and even compulsory) administrative formality in a large number of countries is, after the tax sector, the most frequently mentioned online administrative procedure, 6 countries indicating offering such a service[2] which is also associated, in 3 countries (Spain, Finland, Norway), by the possibility to consult one's file on line. These services are applied a variable level of security from a country to another, some of them (Spain, Finland) implementing an electronic signature system.

3. The next online procedure quoted is job research, also implemented in 6 countries[3], which is sometimes supplied with the possibility of on line consultation of one's file (3 countries). These procedures are generally accessible by login and passwords, therefore by traditional safety procedures.

   A whole list of other on-line procedures were also mentioned, such as the requests for building permits, loans in public libraries, the requests for documents from the Registry Office, the registration procedures for new companies, the social taxes, users' relations with health institutions professionals, registrations in schools and universities, registrations for exams, car registration, reimbursement of medical expenses and finally registration of complaints (police, justice…), this last service being generally associated to a mailing service.

   The analysis of the answers brought by data protection authorities on the security of the previously mentioned procedures show a great disparity of situations, except for some services, undoubtedly considered more "sensitive" (ex: car registration, validation of the reimbursement of medical expenses, etc.…), and which seem to attract specific security measures. No significant conclusion can thus be drawn except for indicating that up to now no country - except perhaps for Finland and Denmark - has a clear vision on the safety requirements to be put into place concerning e-government applications.

C. INSTITUTION OF A UNIQUE ENTRY POINT TO ONLINE ADMINISTRATIVE PROCEDURES, OR "PORTAL"

1. General

The "portal" approach, i.e. the development of a unique entry point to online administrative procedures, exists or is envisaged in almost all the countries concerned with this study. This general tendency appears in the countries where the development of sites more or less playing the role of independent portals as well as in the countries where no system pre-existed.

In some cases, a specific ministry is in charge of this portal. Thus, in Finland, site http://www.suomi.fi is managed by the Ministry of Finance; in Austria, the portal of the Federal Government http://www.help.gov.at is also managed by the Ministry of Finance.

---

2 Denmark, Spain, Finland, Italy, Norway, The Netherlands.

3 Denmark, Finland, France, Italy, Norway, Portugal.

These portals generally constitute sites of general information: links towards the various public and institutional services; directory of the addresses of administrations and public institutions; information files; excerpts from the Official Journal concerning various procedures (forms; information on administrative procedures; information on financial help, requests for funds, invitations to tender, jobs offered in the public sector, etc.); information on national legislation; current events; "box of suggestions"; publications, etc.

More and more frequently, these portals are also used to have access to on line administrative procedures, concerning both citizens and companies. Thus arises the issue of the possible retention of personal data on the portal. At present, these sites would not retain personal data in Denmark, Germany, Spain, Portugal and Sweden. However, such sites can or will be able to retain such personal data in Belgium, Italy, Norway, Finland, Austria (exclusively if the citizen is about to enter a procedure absolutely requiring identification) and Ireland.

In this last country, the system will provide for registration on-line. It consists of identity authentication by way of a person's Public Service Number (PPSN) and the provision of Government services through a Broker which will hold personal data in a secure central data vault. A person's identity will be authenticated by the Public Service Identity Database, which contains basic identity details, operated by the Department of Social and Family Affairs. The system will provide for additional authentication requirements for more secure and confidential transactions.

Access of services through the Broker will be based on individual consent and a member of the public will not be required to use the system in order to access services. Frequently used personal data (e.g. birth and passport details, income, family relationships etc) will be held by the Broker in a central data vault. The Broker will manage this information and protect it for the user. Relevant data will only be released to a public service agency on the specific instructions of the user in the course of a transaction for a service via the Broker. Appropriate security policies for different services will be developed and the personal data in the vault will be encrypted.

When developed, it will be possible for the Broker to anticipate life events (e.g. pension) and each category of the system will have the "intelligence" to suggest the points of interest or relevance for the person. The Broker, through the portal, will provide a "one-stop shop" for persons transacting Government services. It will progressively allow the personalisation of the particular services as a profile of successive visits will be built up. The position of the Government is that the private life of the user is respected as the user will have given his consent for his data to be used and stored in this manner for the provision of the particular service. This model was approved by the Irish Authority, subject to strict Data Protection conditions relating to consent and use of data for particular purposes".

The Dutch Authority also discussed the point, by drawing the attention of the administration to the impact in terms of data protection of the operational distinction between "front office" and "back office", i.e. the services of contact with the citizen on one hand (counters and Reception Offices), and the services of file handling on the other hand. The "front office" administration collects all kinds of data necessary to the supply of the services required by the citizen, the administration of "back office" then will use

these data so as to appreciate the position of the citizen as to each one of these services; thus, the administration can provide a single counter so as to provide several services. The administration increasingly tends to resort to this organisational structure, whose services of portal and "unique counter" are emblematic. In its annual report, the Dutch Authority insisted on the fact that administrations must, in these circumstances, strictly define the respective responsibilities of each department concerned according to the data processed, in order to prevent any unlawful use or circulation of the data of the citizen within the "back office" services.

2. Recourse to private external providers that can store or have access to the user's personal data

The proximity between the electronic government and the on line commercial procedures and, consequently, the possibility that on line administrative procedures are provided by private companies, impose to consider various elements relative to the technical organisation of electronic government services. For instance, how can private companies ensure equality of treatment in public procedures; how are they remunerated; does that imply that certain on line administrative procedures should not be free, etc?

These questions did not attract the same answers in the various countries of the European Union.

Thus, the choice not to turn to private providers that may have access to the users' personal data was retained in Germany, in Italy, in Spain, in the Netherlands, in Sweden and in Norway. In most of these countries, however, and notably Spain, the public authorities have recourse to private external providers for purposes of product or portal development, for instance. In Spain, furthermore, private operators are also called to cooperate to carry out audit plans in relation with the development of portal planning.

The opposite choice was made in Belgium, in Denmark, in France (only occasionally), in Finland and in Austria, where any eligible private provider can apply for recognition after having proved that he will implement the necessary guarantees for safety, especially concerning data protection. No certainty exists on this point in Portugal and the United Kingdom, where in this framework, there would however not be any objection of principle to the fact of turning to private external providers.

No country would have implemented the Passport service offered by Microsoft within the framework of electronic government projects, certain Authorities having no specific information on the matter.

3. Opinion of the Authority on these subjects and reaction of the government

Not all Data Protection Authorities have had to deal with questions relating to the institution of a portal in their country, notably because the projects in place do not always imply that data is registered by the portal.

On the contrary, in the countries where the portal implies processing of personal data, the Authorities answered by insisting on the fact that turning to external providers could be envisaged only once the specific guarantees will be implemented. Thus, the multiple requirements resulting from the recommendations of several authorities mention the following guarantees: adequate contract with data processors; precise determination of

the missions of external private providers; determination of security requirements (protected and entirely automated environment); compliance of private external providers with specific legal requirements (accreditation) including in particular the prohibition to use the data for other purposes than the original ones for which they were collected, or prohibition to disclose these data; precise determination of the data registered; possible set up of an inspection committee, etc.

D. NATIONAL SYSTEMS OF INDIVIDUALS' IDENTIFICATION (USE OF UNIQUE OR SECTOR-BASED IDENTIFIERS TO HAVE ACCESS TO CERTAIN ON LINE ADMINISTRATIVE SERVICES)

At first, it is useful to recall that until now, the only countries having implemented a unique and general identifier at the national level are Belgium, Denmark, Spain, Finland, Ireland, Italy, Luxembourg, Norway and Sweden. Projects of development of such unique identifiers exist in other countries, in particular in Austria, but only as a hidden source number for sector-based identification numbers (see below). In Denmark, Belgium and Spain, this unique identifier coexists with sector-based identifiers. In the remaining countries, only sector-based identifiers exist: Germany (social security, passport number), France and Portugal (essentially social security number), Greece, the Netherlands (social-tax identifier, in particular). In countries like Germany and Portugal, it is relevant to recall that recourse to a unique identifier is considered as unconstitutional.

The development of e-government sometimes constitutes the occasion to redesign this system of identifier or to extend the range of a sector-based identifier. At present, only in Portugal and in Austria is it indicated that these developments involved an overhaul of their national system of identification of the people.

1. The general tendency is, for the purpose of access to online administrative procedures, to have recourse to pre-existent identifiers, whether unique (Belgium, Denmark, Spain, Ireland) or sector-based (France, Netherlands, Portugal, Italy). In some of the countries where unique identifiers do not exist, it was sustained that the implementation of a personalised portal by the administration should not constitute an occasion to implement such a unique identifier (France, in particular). Austria offers a particular case in this respect, as it is about to create a unique identification number (the Residents' Register number) which must not be stored outside the Residents' Register and is only used for the delineation of sector-based identifiers by means of a specially protected procedure. No public authority is allowed to store identification numbers of a sector outside its remit.

2. Projects of extension of sector-based identifiers for the purpose of access to online administrative procedures were, or are still considered in certain countries. A project of generalisation of the social-fiscal identifier in the Netherlands was given up by the government, following the negative opinion of the Authority on this point. At present, such a project only exists in Italy, where it is expected that the tax identifier will be generalised to constitute a unique identifier to have access to certain online administrative procedures. In Ireland, the PPSN ("Personal Public Service Number") is a statutory unique identifier for accessing public services and, pursuant to the legislation, may be

used for tax and social services as well as other public and local authority services.

3. A debate incidentally took place in Italy on the risk of *de facto* generalisation of a sector-based identifier (in this case, the Italian fiscal number) once integrated into an electronic identity card: the Italian Authority reminded government that under the terms of article 8 (7) of Directive 95/46, concerning the institution of a unique identifier, it was advisable to strictly determine the conditions under which such a number would be used for treatment. The Italian government assured the Italian Authority that it intended to take this opinion into a account, but at present the situation is not definitively fixed.

4. The liberalisation of the use of the single identifier is effective in Ireland, and is expected in Belgium. In Belgium, the use of the national register number (and by default for persons not holding a national register number, the social security identifier) as unique identifier is from now on compulsory in all the information systems of the public authorities. The Data Protection Authority must give an opinion on this question in an imminent way.

5. Recourse to sector-based identifiers only is maintained in Germany, Portugal, the United Kingdom and France. These sector-based identifiers will then be used only for their original purposes.

6. Following the same logic of avoidance of interconnection risks, other Authorities claimed or suggested that one should turn to derived sector-based identifiers, in particular in the Netherlands, where the preliminary draft of the government was thus modified, and in Austria, where the (hidden) unique identification number combined with the electronic signature in a special function (the so called "Bürgerkarte" or "Citizen Card") will be used for securing online access to all e-Government applications and even specially structured online applications in the private sector.

7. Specific :

    - In Finland, a project of review of the systems of identification of individuals in the context of e-government is envisaged, which implies to have recourse only to a unique identifier specifically created for the purpose of electronic signature and electronic identification for the population register centre. It is not expected that this identifier will be used to have access to on line administrative procedures. The pre-existing unique identifier, the social security number, should not be used for these purposes.
    - In Belgium, the development of e-government was the occasion to create a unique identifier for businesses: The current VAT number (extended to companies and organisations non subject to the VAT) is converted into a unique identifier for all businesses and organisations; this number will replace all the other specific numbers and will be introduced as unique identifier for companies and organisations for all the information systems of the authorities.

E. INTERCONNECTIONS IMPLIED BY THE DEVELOPMENT OF E-GOVERNMENT

A particular concern, expressed in a vivid way by the British Authority, is that the development of e-government should not operate as a smokescreen hiding a generalised interconnection of public information databases and an increased exchange of personal data between administrations. The CNIL also recalled its general doctrine, which consists in refusing any generalised interconnection of the files. The CNIL recalled this position on the occasion of consultations organised by the authors of a report, written upon the request of government, on "e-government and protection of personal data". Following the delivery of this report to government, a public discussion was organized on the main points identified during its drafting. One of the main conclusions of this public discussion, going perfectly along the same lines as the CNIL's doctrine, was that e-government should not result in an increase in the level of control on the individuals, this control resulting firstly from interconnections.

In addition, in Germany, it is significant to stress that it is just about the issue of interconnections that the German Supreme Court retained its famous theory of the individuals' "right to informational self-determination". This right consists, for each individual, in being able to decide the communication and use of his/her data by third parties. The recognition of this right, if it does not amount to an absolute ban of interconnections, at least limits much the possibilities of interconnections.

In this respect, when it was mentioned in some countries that interconnections were envisaged, the essential motivation of this development resulted from a desire of simplification of procedures. This motivation concerns companies as well as individuals, in particular, concerning the latter, at the occasion of change of address. The objective to fight fraud was also mentioned (in particular in Ireland and in the United Kingdom)

At present, these interconnections are generally not defined, or are only in the course of definition. The fields concerned vary according to national concerns: among others it is possible to mention the health sector (Spain, Finland), the management of the relations between administrations and companies (Belgium), the indexing of public files (Italy), the implementation of procedures of information within public administrations (Spain: this specifically refers to the so-called Single Window, which permits coordination between various administrative departments in the course of proceedings based on the exchange of documents).

Several Data Protection Authorities take part in working groups where these questions are examined (for example in the Netherlands or in Finland); others, like the CNIL, deal with these issues as a consequence of their power of prior checking of the processing of personal data in the public sector.

The questions relating to these projects are systematically the same in all the countries involved:

- At the legal level, interconnections are handled either within the framework of an authorisation by statute (France), or within the framework of provisions requiring the persons' consent. Thus, in Spain, the DPA considered the project of regulation on the promotion of e-government as compliant with the requirements of the general data protection law, by requiring the consent of the people concerned before the transfer of the data by electronic way between

administrations. This regulation was adopted by Royal Decree of 28 February 2003 relative to the regulation of telematic registers, notifications, certificates and transmissions. This Decree also establishes the procedures that must be used to use these systems, in particular in the context of communications with citizens or for the exchange of information within public departments. In the last case, therefore, prior consent of the data subject is required. It is worth mentioning also that the Decree contains a clause imposing an obligation on the public administration to comply with the Data Protection Act.

- As for the principles of protection, countries particularly insisted on the principles of quality of the data, of legitimacy of the processing, information to the persons concerned, as well as on the safety level implemented.

The questions relating to the need and the general conditions of implementation of interconnections were specifically considered in the United Kingdom on the occasion of the publication, in 2002, of a report ordered by the British government to the "Performance and Innovation Unit" (an organisation of strategic thinking at the heart of the British government, from now on called “Strategy Unit”). This report entitled "Privacy and data sharing: the way forward for public services ", presents the matter of interconnection as seemingly promoted by the development of e-government and the expectations of the citizens in this field, but insists on the equivalent relevance of their expectations as for the protection of their privacy. Thus it is important to set a balance between interconnections (and the consequently supposed improvement of the services of the administration) and the protection of the users as regards the processing of their personal data. The search for this balance would obligatorily have to go through the following steps of analysis:

- what are the expected advantages of the use of the data and their interconnection considering the objectives of the government;
- are there any alternative approaches to achieve the same goal;
- what are the risks and the costs induced by an interconnection;
- what could be the necessary guarantees to manage these risks (ex:ample: PETs);
- at the end of this analysis, is there a balance between the benefit and the risks induced by the interconnection considered.

Last but not least, one of the essential interests of this report is to remind that interconnections are not inevitable to improve the services of the administration.

F. ELECTRONIC SIGNATURE AND PUBLIC KEY INFRASTRUCTURE

The majority of the delegations indicate that in the countries concerned the participation of private operators, "certification service providers" is, or would be allowed within the framework of the implementation of electronic signature mechanisms for certain online administrative procedures. In these cases, the statute of certification service provider is legally framed (for example, condition of agreement). These issues were frequently settled at the time of the transposition in national law of the Directive on electronic signature.

In the remaining cases, recourse to private external providers is impossible, owing to the fact that the State only ensures this role (Germany, Spain). In France, this role operates by default: up to now private external providers operate only in the context of

certification of VAT on line declarations. In all other cases, the State plays the role of authority of certification.

In general it is stressed that recourse to mechanisms of electronic signature is not much developed at present, either because of the absence of appropriate legal framework, or because the costs and the complexity of these systems are still too high. Thus the CNIL underlines, in this respect, that systematic recourse to such processes cannot constitute a prerequisite to the implementation of online administrative procedures: in the current state of the law, of the art and of the market of public key infrastructure, it would be premature to impose such a requirement. On the contrary, it is mentioned that certain administrative procedures are not yet on line because they would require the implementation of means of electronic signature and of encryption. Thus, with certain exceptions, many administrations still have no public general procedure to which is associated a mechanism of electronic signature. One such exemption is Denmark, where electronic signature mechanisms have already been developed. Thus electronic signatures for citizens are handed out free of charge and many internet portals are made ready to provide e-government services.

The fields of these applications express variable priorities according to countries: tax and social sectors (France), register of the population (Finland), for example. In the majority of the cases, these mechanisms equally relate to individuals, companies and agents of the administration. Sometimes the individuals are the first concerned (Germany), sometimes employees, the organisations and servers, and thus not mainly individuals (Denmark), sometimes the agents of the administration are the first concerned (Norway). A distinction was recalled on this last point: electronic signatures concerning public agents do not so much require to identify the individual behind the signature as to identify whether the person behind the signature has the necessary abilities to make a decision or to carry out the action concerned.

Data Protection Authorities could inform the public authorities on their positions on various occasions. Sometimes they were consulted by government on the occasion of the adoption of statutory or regulatory measures on the framing of activities requiring the implementation of electronic signatures; sometimes they decided to give their opinion following the submission to their prior examination of particular applications.

The general attitude of Data protection authorities towards mechanisms of electronic signature is positive, because those are interpreted as mechanisms likely to support personal data protection. However, several of them have stressed the relevance to include questions of data protection in the development of these mechanisms. It was in particular recommended that clear information must be provided to the user by certification service providers on the communication of data, in compliance with the rules on the communication of personal data. Also a clear, unique identification of persons requesting online access to personal data is considered by the Austrian Data Protection Commission as an important contribution to data protection in the framework of e-Government.

G. ELECTRONIC IDENTITY CARDS

1. At present, sector-based cards constitute the majority of the electronic identity cards held by individuals in European countries. These sector-based cards mostly are social security cards, on which it is occasionally envisaged to register health data in the long term (for instance in Austria). These sector-based cards

sometimes coexist with general identity cards, in particular in Belgium and Finland.

2. Eventually there should be as many countries having implemented general ID cards as countries having implemented only sector-based cards. Indeed, if general electronic identity cards were delivered at present only in Belgium, Italy and Finland, this delivery is expected in Germany, Sweden, France, Spain and the United Kingdom (where one talks of "entitlement cards": the card would not be used for identity checks, but to identify persons willing to have access to certain online administrative services and would also constitute a social security card). In Portugal, a unique card is also in project. It would record various types of data on a single card, which would correspond to various identifiers, one administration being able to have access only to the data by which it is concerned. A study on the technical feasibility of this card is in progress. The Portuguese Data Protection Authority requested to be informed on the evolution of this work, in order to guarantee the respect of the constitutional provisions prohibiting the institution of a single identifier in Portugal.

3. The experiences where the most advanced projects of electronic identity cards have been implemented in Italy and Finland.

   - In Finland, the electronic identification card consists in an identity card including the photograph of his/her owner and a chip on which are recorded the holder's authentication certificate, the certificate of non repudiation necessary for the applications of electronic signature, and the certificate of the Population Register Centre, which will deliver the "e-number" of the person. This single number is primarily used for the purposes of commercial transactions. The card contains no information on the universal identifier of the person (determined at birth), neither his/her address nor his/her date of birth. It is secured by a personal identifier (PIN), which the user can also use to have access to information networks such as the Internet. On top of being an identity card (as well as a passport or a driving licence), this card is also useful for electronic identification and electronic signature purposes. It is useful in the context of commercial transactions, but also in relations with the administration. Thus, for example, the card can be used to validate a change of address on line by using the application created for this purpose by the Population Register Centre and the Finnish Post office. In November 2002, in addition, the government proposed that this identity card is associated to the social security card. Upon the Data Protection Ombudsman's request, it was mentioned in the project that the person remains free to decide if social security and health data were to be integrated into the card.

     At present, the card costs € 29 and is valid for 3 years; it is envisaged to increase the costs up to € 40 and to extend the period of validity up to 5 years. It is not only delivered to Finnish citizens: foreign individuals living permanently in Finland and whose identity could validly be proven can also become titular of a card.

     These cards are delivered by the local police agencies upon presentation of an identity card, passport or driving licence. The Population Register Centre,

which is used as certification service provider by the Finnish administration, provides the necessary certificates for electronic identification. In addition to the card, a smart-card reader is necessary, which the users must hold at home. However, the identification would eventually be possible from a mobile device, such as a portable phone, equipped with a special chip. A system of declaration of loss or theft is available around the clock.

The Finnish identity card did not meet with the expected success. At present, only 13.000 Finns have adopted it. Among the main factors explaining this lack of popularity, are evoked the fact that the card is not free nor the smart-card readers which the users must hold at home to use the card for purposes of commercial transactions on the Internet, and a relatively fuzzy perception of the benefit induced by its detention. Thus, the establishment of the card being optional, the Finns generally preferred to stick to the traditional identity papers.

- The Italian electronic identity card, as opposed to the Finnish one, is intended to replace the identity card paper and would be thus compulsory for every citizen. According to the current project, in addition to the fact of being an identity card in the strict sense, as well as a title of nationality and a title authorizing free movement within the European Union, the Italian identity card would also give access to the national and local public services; it would also offer a function of electronic signature and would allow citizens to vote on line. Other functions could be offered, such as the possibility to make appointments on line with a doctor, for example.

  This card which can be issued to minors, contains identity data but also the tax identifier of the person. In the long term it will contain the fingerprints and the health data of the person (except DNA), the registration of which its holder will authorize (this requirement of prior authorisation by the person was implemented following the intervention of the Italian Data Protection Authority). The government intends to promote the use of the card on the Internet by installing terminals for the public in bars, restaurants and shops, the electronic identity card then having a function of on line identification. Another objective of this action is that shopkeepers can play the role of administrative counters, which would in the long term allow to reduce the costs of these operations for the administration.

  Among the concerns of the Italian ministry of the Interior for the implementation of this project, one finds, among others, the concerns to centralise in a logical way authorisations of issuance of the card, to guarantee the independence of the local communities in the implementation of their on line services with the citizens and to implement a security policy for the card itself, at the time of its issuance and throughout his life cycle. This security policy consisted for example, in defining a complex process of production, initialisation, activation and issuance of the card, the latter being produced by the local authorities having the function of collecting the personal data and of registering them on the card, including the photograph.

  The card uses two technologies on a traditional plastic medium: a micro processor of 16K and a laser band. On the plastic card would be visibly

registered a photograph, the name, first name, sex, date and place of birth of the person as well as a unique identifier. On the other side the address and the number of tax number of the person, the period of validity of the card would be registered, as well as two components would be embedded (the microprocessor and the laser band). Information on the person, as well as his/her fingerprint and his/her signature would be found in hologram on the laser band also.

Both technologies each have their raison d'être: the laser band is used as identity card and the microprocessor as services card. The microprocessor would ensure identification and authentication purposes on the basis of symmetric and asymmetric keys. It would be possible to store up to sixteen keys on a card.

4. When projects of general electronic identity card exist, their purposes are generally common.

   First of all, they are obviously used as certificates of identity of the person.

   1. It is also nearly systematically envisaged that this card can be used to have access to online administrative procedures (except in Germany, according to the information currently available), to be identified and to authenticate oneself in e-trade transactions (this point being still undefined in Spain).
   2. The function of electronic signature is systematically envisaged, for online administrative procedures as well as for e-trade applications (this last point being however still undefined in Spain).
   3. On the other hand, these cards may be used as pay cards only in Germany, Italy, Austria, Portugal and Sweden.
   4. The "health card" function is definitively retained only in Germany and Finland, and it is considered in Portugal, in Italy and in Austria.
   5. The "social security" function is retained only in Germany and Finland. In the other countries, it is frequent that a sector-based card plays this role.
   6. Finally, these cards would also be used as voting cards in Germany, Italy, the Netherlands, and potentially Portugal and Sweden.

5. Most European Data Protection Authorities were consulted on these issues. Some approved the projects envisaged by the public authorities (Finland, Sweden), others are currently discussing existing projects, others have supported different opinions from those of the administration in charge of the project (Italy, the Netherlands). In any case, several elements were raised as potentially problematic:

   1. Determination of the nature of the data registered on the card,
   2. Determination of the procedures of data processing,
   3. Determination of the organisations allowed to have access to the various categories of information,
   4. Respect of the individuals' rights,
   5. Determination of the administrations entitled to decide of the nature of the data registered in the electronic identity card,
   6. Potential use of the electronic identity card for commercial purposes (on line payment, electronic wallet, etc),

7. Security measures implemented (Italy underlining in this respect that today, only one company in the world would be able to offer solutions at the level of the technological ambitions of the project),

Central storage of health and biometric data (fingerprints).

H. CONTROL OF THE USER OVER HIS/HER PERSONAL DATA

This point is not solved identically in the various countries of the European Union. Actually, as the British Authority indicates, there can be tensions within the administration between the desire to provide coherent and practical services for the user, and the wish to combine sources of information on the people, in a way likely to constitute an infringement of data protection legislation. The control of their personal data by the citizens is thus at the heart of this tension. To read the answers of the Authorities on this point, there are two main tendencies on these questions:

A first tendency, to which several countries subscribe expressly, generally with the agreement of the Data protection authorities (Ireland, Denmark, Spain, Finland), consists in considering that citizens must keep their data under control at all stages of the administrative procedures, and that they must have an information feedback on the data exchanges having underlain any decision taken about them. A consequence of this tendency is that data exchange between administrations by telematics can be subjected to the consent of the persons concerned (ex: Spain, Ireland). In other countries the situation is more hesitant (United Kingdom, Belgium). This first tendency is supported by the opinion that such a personal control would condition the confidence which e-government must generate, as well as its credibility. In the same way, as a snowball effect, the more the citizens rely on their administration, the less they would need to exert such a control.

However, even if the user retains control on his/her data, the fundamental principles of data protection must also be applied. Thus, in order to satisfy the condition of the fair collection of data, the Irish Authority recommends not to feed the database by using data already supplied for a different purpose. Instead, it was recommended and accepted that citizens would be given an opportunity to consent to their inclusion in the new system and to be informed about the purposes and uses of the central database. The principle of quality of data also has to be respected: thus excessive or irrelevant personal data, which are not likely to have a legitimate and relevant public service application, should not be asked for or stored. The individual should be free to determine which additional data he/she wishes to provide in order to avail of a wider range of services. In the same way, individuals must be aware of the range of potential uses of their data at the time of their collection, and administrative agents should be clearly informed about the forms of legitimate use of the data to which they have access. This information must thus be sufficiently precise so that the persons can really understand the potential risks and the consequences induced by the transmission of their data. In the absence of such information, the person's consent would be an illusion, because it would not have any justified reason to refuse the communication of his/her data vis-à-vis the argument of simplification of administrative procedures.

What is more, several Authorities also underline that another key point consists in ensuring a satisfactory level of security of the applications concerned. This point is not theoretical, as a recent opinion of the Spanish Authority shows. In the case at hand, a local authority had sub-contracted to two financial organisations the implementation of a request procedure for certificates of residence, used by the applicants to obtain rebates on

public transport tickets. The financial organisations issued these certificates by using the ticket delivery machines. However, during the request procedure, the ticket delivery machine made it possible to visualise not only one's own personal data, but also those of the persons living in the same residence, who were also registered in the database. The Spanish Authority sanctioned the local authority for illegal disclosure of the data.

On the contrary, a second tendency consists in considering that administrative simplification necessarily operates at the price of a certain loss of control of the user's own personal data. One could thus not satisfy at the same time the requirements of faster e-government and the requirements of "traditional" information of the citizens. Three countries (Portugal, Germany and Italy) consider that the control of citizens on their data is not a necessary consequence of the development of e-government. An argument raised by the French Authority, in this respect, is the risk that this control is often only an illusion in practice. Indeed, the user would wrongly think he/she controls his/her data, whereas the administration obviously constitutes a field of intervention where individuals can be forced by law and regulations to provide data to the administration. In the same line, the Portuguese DPA considers that, even though e-government may support partially the person's right of access to their data available on line, the user would not exert any further control on their data, in particular when it comes to the data subject's consent to the communication of his/her data to third parties within the administration**.**

I. ESTABLISHMENT OF A CONTROL AUTHORITY ON DATA PROTECTION SPECIFIC TO THE PROJECTS OF ELECTRONIC GOVERNMENT

Except in Belgium and, to a certain extent, Finland, the question of the setting up of a specific Data Protection Authority for e-government issues has not been raised at all. The pre-existent Authorities seem to be naturally dedicated to be the competent Authorities to give opinions on e-government projects having an impact in terms of data protection.

Other authorities than Data Protection Authorities can be called to consider data protection issues in the field of electronic government. Thus, for example, in the United Kingdom, the Government Ombudsman can investigate complaints of individuals concerning the activities of the administration, including e-government activities. In the same way, in Finland, the telecommunication regulation authority remains in charge of checking the compliance of certification authorities and telecommunications in general, as well as the questions of electronic filing come under the field of competence of the corresponding administrations. Sometimes, as in Denmark, the Data Protection Authority expressly took additional competences at the public authorities' request, concerning the authorisation of security solutions in the field of e-government. In all these cases, at any rate, the point does not consist in splitting a competence of checking compliance of these activities the data protection legislation between Data Protection Authorities and another authority.

On the other hand, this split in competence has been considered in Belgium. A project is currently in hand, which consists in establishing an Audit Board, other than the Data Protection Authority, which would consist in authorisations committees of access to non-public data held by the administration in the database called "business databank" ("banque carrefour des entreprises"). At first, these authorisation committees were to be distinct from the Commission. The latter, in its decision relating to the institution of the base, demanded that these committees should be established within the Commission itself. It specifically stressed that the creation of distinct commissions causes prejudice to

the necessary unity of approach which should characterize, at the institutional level in particular, the control of the respect of privacy. Thus the Belgian Commission reminded government that it considered as crucial that the consequences of this choice at this time were well evaluated at the time when Government intended to develop an e-government policy, including all the applications that e-government will have in the future in all sectors of the administration, such as for example the electronic identity card. Considering the increase in such questions to be reasonable expected, the Commission considered as significant that the questions related to the fundamental rights and freedoms of the citizens generated by the institution of this new database should be studied, as far as possible, by one single institution. In the current project, these committees would from now on be established within the Commission. They would be committees made up of a certain number of Members of the Commission, accompanied with representatives and/or experts of the related sectors.

Done at Brussels, on 8 May 2003
For the Working Party
The Chairman
Stefano RODOTA