



*Présidence luxembourgeoise
du Conseil de l'Union européenne*

Ministère de la Fonction publique et de la Réforme administrative

Centre de Recherche Public Gabriel Lippmann

**Interoperability of eGovernment systems
The identification number,
data sharing and data protection issues**

Luxembourg, June 2005



**Centre de Recherche Public
Gabriel Lippmann**

Survey for the 44th meeting of the Directors general responsible for Public Administration of the EU member states

Content list

1.	Introduction	7
1.1.	General remarks	7
1.2.	Composition of the questionnaire and aims	7
1.3.	Identity, data sharing and data protection	8
1.4.	Structure of the report	9
2.	General Summary of the results	11
2.1.	Countries having participated at the survey	11
2.2.	The existence of a single identification number.....	11
2.2.1.	Questions I.1-2: Existence of a SIN and sector specific identifiers	11
2.2.2.	Question I.3: Alternatives if there is no SIN	14
2.2.3.	Question I.4: Plans to change the current situation	14
2.3.	Technical aspects of the single identification number	15
2.3.1.	Question II.5: Technical construction of the SIN	15
2.3.2.	Question II.6: Data linked to the SIN.....	16
2.4.	Organisational aspects of the SIN	16
2.4.1.	Person subgroups covered by the SIN (Q III.7).....	16
2.4.2.	Public authority responsible for management of SIN database (Q III.8).....	17
2.4.3.	Registers accessing the SIN data and documents comprising the SIN (Q III.9) 17	
2.5.	Legal issues	18
2.5.1.	Laws brought into force to comply with the directive 95/46/EC.....	18
2.5.2.	Authority monitoring the application of Data Protection legislation.....	19
2.5.3.	Processing of Personal Data: Obligation to notify the authority.....	19
2.5.4.	Rights of the data subject	20
2.5.5.	Data sharing between administrations.....	22
2.5.6.	Shared databases	24

2.5.7.	Allowed uses of the Single Identification Number	24
2.5.8.	Present and future of the national situation	25
3.	Conclusions	29
A.	Annexe : Country Summaries	33
A.1.	Austria	33
A.2.	Belgium	34
A.3.	Bulgaria	35
A.4.	Cyprus	36
A.5.	Czech republic	37
A.6.	Denmark	38
A.7.	France	39
A.8.	Germany	40
A.9.	Hungary	41
A.10.	Ireland	42
A.11.	Italy	43
A.12.	Lithuania	44
A.13.	Luxembourg	45
A.14.	Malta	46
A.15.	Netherlands	47
A.16.	Poland	48
A.17.	Spain	49
A.18.	Sweden	50
A.19.	United Kingdom	51
B.	Annexe: Synoptical tables	53

Foreword

This report results from a study carried out by the '*Cellule de Recherche, d'Etude et de Développement en Informatique*' (CREDI) of the '*Centre de Recherche Public – Gabriel Lippmann*', on behalf of the '*Ministère de la Fonction Publique et de la Réforme Administrative*' on the occasion of Luxembourg's presidency of the Council of the European Union during the first six months of 2005.

First of all, we would like to warmly thank all the countries having answered to the questionnaire that we sent them in the beginning of 2005. Without their participation, this study would not have delivered any result.

The constructive collaboration of several Luxembourg authorities also needs to be pointed out. We would like to mention especially in this context the fruitful contribution of the '*Commission Nationale pour la Protection des Données*', the '*Centre Informatique de l'Etat*', and, obviously, the '*Ministère de la Fonction Publique et de la Réforme Administrative*'.

We hope that this report will contribute to a better understanding of the European situation concerning the identification number, data sharing, and data protection issues.

Benoît Otjacques, Deputy Scientific Director CREDI

Patrik Hitzelberger, Project Manager CREDI

1. Introduction

1.1. General remarks

This report summarises the results and conclusions drawn from a study realised for the EPAN working group eGovernment during Luxembourg's Presidency 2005. As the title makes clear, the general topic of the study is the interoperability of eGovernment systems. It is self-evident that this field is much too complex and voluminous to be treated exhaustively by the limited resources dedicated to this study. Nevertheless, the fact that the study focuses on identification handling in the EU and relates it to data sharing and data protection issues might be regarded as an advantage, since these questions are crucial and emerging topics in the area of interoperable eGovernment systems. Specifically the cross-border, pan-European exchange of personal data is a challenge that is influenced tremendously by these issues.

Besides the fact that identity management in general is without any doubt topical, and that the relation to data protection adds a new aspect, there was a second major motivation for conducting the survey. In the study "The Electronic Identification of Citizens and Organisations in The European Union: State of Affairs", carried out by EIPA during the Belgian presidency in 2001, identification management has already been illuminated.

It goes without saying that four years in E-Government are a rather long period – and that with the accession of the ten new member states in 2004 and the current four candidate countries the composition of the Union has changed significantly since then. Consequently, the intention of the Luxembourgish Presidency was to provide an update of the situation drawn up 2001 and to get the new picture for the bigger Union. This update could be accomplished for the identification part of the Belgian part only, because this new study did not take into account all authentication related issues, like for instance electronic ID cards. This idea followed the résumé of the debate in the EPAN WG eGovernment after the presentation of the Belgian study in November 2001, where the members agreed that it was "... necessary for the future debate in this WG to split up the theme of unique id. keys, electronic signatures and electronic id. cards and treat them separately...".

As already mentioned, the study relates the identity management domain to data protection concerns. In this context, the legal base of the Directive 95/46/EC and its national implementation has been of special interest.

1.2. Composition of the questionnaire and aims

As pointed out above, we have analysed the current situation in the member states and candidate countries regarding the way these states identify their citizens (and other subgroups of natural persons) and legal persons. We were particularly interested in the procedures and technical details of all national systems that use a "unique" or single identification number (hereafter *SIN*) for this purpose.

To be more precise, the questionnaire consisted of four parts

- Section I: Existence of a single identification number
- Section II: Technical aspects of the single identification number
- Section III: Organisation aspects of the single identification number

- Section IV: Legal aspects

As regards sections I through III, we have adopted most of the questions already posed in 2001 (with some slight modifications), since the study aimed to obtain an update of the Belgian results and to take into account the new member states and candidate countries.

It is worthwhile noticing that the focus of the Belgian study was also on *electronic* identification, whereas we have restricted the scope to the existence of an identifier, its technical realisation and the related data protection questions.

We have also evaluated future plans in the area of identity management and data protection, since this will have an impact on almost all data sharing applications in the eGovernment area.

It goes without saying that the *political* discussion about identifying individuals has changed significantly since the year 2001. We have confined ourselves to evaluating and observing the European status quo of identity management and data protection application in this area, and do not make any political statement.

Summing, this study has focused on the eGovernment subject of the EPAN WG , meaning that it describes the actual and future way in which the European countries identify their individuals and organisations.

1.3. Identity, data sharing and data protection

This report cannot provide an extensive explanation of the subject “identity” or “identity management” in eGovernment.

Nevertheless, it should be underpinned that quite often, when there are discussions and debates about identity in IT related domains like eGovernment, two different aspects of the issue are somewhat admixed:

- The reduction of a “real” individual or organisation to a very limited set of data and a identifying key for this data, together with the necessary procedures and technical infrastructure to manage this, and
- The ways and means an individual or organisation can evidence his/her or its identity, for example when authenticating to use eGovernment systems.

Within the scope of this report, only the first aspect has been investigated. In this sense, we define “identity” as

a (technical) concept of representing individuals and organisations by a data set and its key(s).

In the latter field, i.e. the authentication domain, solutions available are based on “what you know” (i.e. PINs + password) or “what you have” (ID cards etc.) or combinations of these approaches. Currently, identification based on biometrical data (hence “what you are”) is becoming more important. Although technically and organisationally challenging, the authentication related questions can be treated independently from the basic “infrastructure” question of identity and its management in the public sector.

To understand better the related, but independent areas, figure 1 shows a graphical model of an simple identity concept and how it is created in terms of IT systems (restricted on a natural person – same principle applies for legal entities).

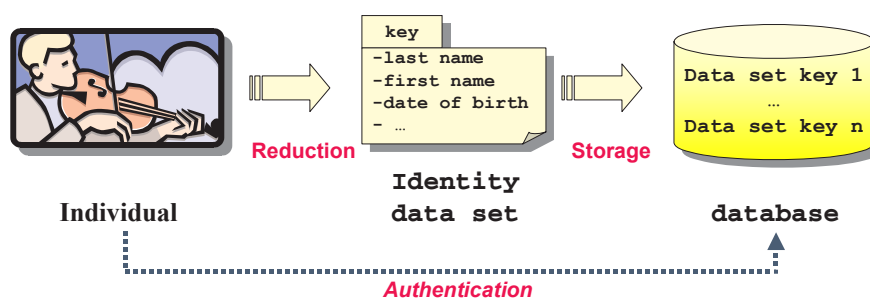


Figure 1: Creating identity from individuals

As the schema shows, there is a strong and self-evident reduction of complexity when representing an individual as a data set – neither the fact that a person plays violin nor any other personal characteristics are necessary to identify an individual. Nevertheless, we will see later on in the report that the range of the data fields actually recorded varies a lot from country to country and goes very often beyond the minimum required.

We will use the simplified schema in figure 1 later on as a means to illustrate different national approaches and notions of “identity” and some other concepts.

It is obvious that the mapping of individuals and organisations to registers is a rather “simple” task – meaning that this has been an administrative and technical reality since centuries. Nowadays, the clear challenge when dealing with identities in E-Government is integration – because integration (or interoperability¹) itself can be regarded as the *raison d’être* of the current E-Government research and its applications.

When turning local E-Government applications into interoperable solutions that cross organisational or even national borders, the question of data protection becomes extremely important. It was the second major goal of this study to find out which provisions and regulations have put in place in this special area of “data sharing of identity related data”, and which obstacles and problems exist in this area.

1.4. Structure of the report

This report consists of two major sections:

- Section 2 gives a general overview and an assessment of the results of the study. It is structured in accordance with the composition of the questionnaire.
- Section 3 draws some more general conclusions on the report and its subject.

¹ Regarding the interoperability of E-Government systems, cf. the study of the Irish Presidency 2004: “Key Principles of an Interoperability Architecture”. In this study, the “Citizen Identity Management” is part of the proposed framework.

The annexe presents the profiles of all countries that have answered to the questionnaire, and regroups detailed synoptical tables with the summarised answers to most of the questions can be found in the annexe.

2. General Summary of the results

2.1. Countries having participated at the survey

The questionnaire has been distributed in the beginning of 2005 to all member states of the EU and the four candidate countries Bulgaria, Croatia, Romania and Turkey.

18 countries have responded to the questionnaire. Latvia, Poland and Slovenia have sent some basic information.².

	2001	2005
Countries polled	15	29
Countries having answered	15	18(+3)

A profile for each country can be found in annexe A of the report. This section will summarise and assess the overall results of the study.

2.2. The existence of a single identification number

2.2.1. Questions I.1-2: Existence of a SIN and sector specific identifiers

Section I of the questionnaire treats the mere existence of a single identification number in the member states. As a matter of fact, the questionnaire already presumes the existence of further identification numbers in most countries – based of the Belgian Presidency’s results. In this former study, it was already pointed out that the simple “yes/no”-scheme³ for the results might be not enough to draw conclusions and asses the results.

To understand better the theoretic possibilities and the de facto situation, we give a short overview of different scenarios in the area of identity management. Please note that this section does not yet take into account all data protection related problems, although the different scenarios have an important impact on this legal aspect as well.

² We have tried to extract the questionnaire-relevant data out of the delivered information. Cf. especially the synoptical tables in annexe B.

³ ...which we provide in annexe B nevertheless

Figure 2 shows a common case that is in fact reality in the majority of the investigated countries: The existence of parallel systems of identity numbers – regarding natural persons either with (for most countries) or without (for example Germany and the UK) the additional existence of a so-called “single” identification number.

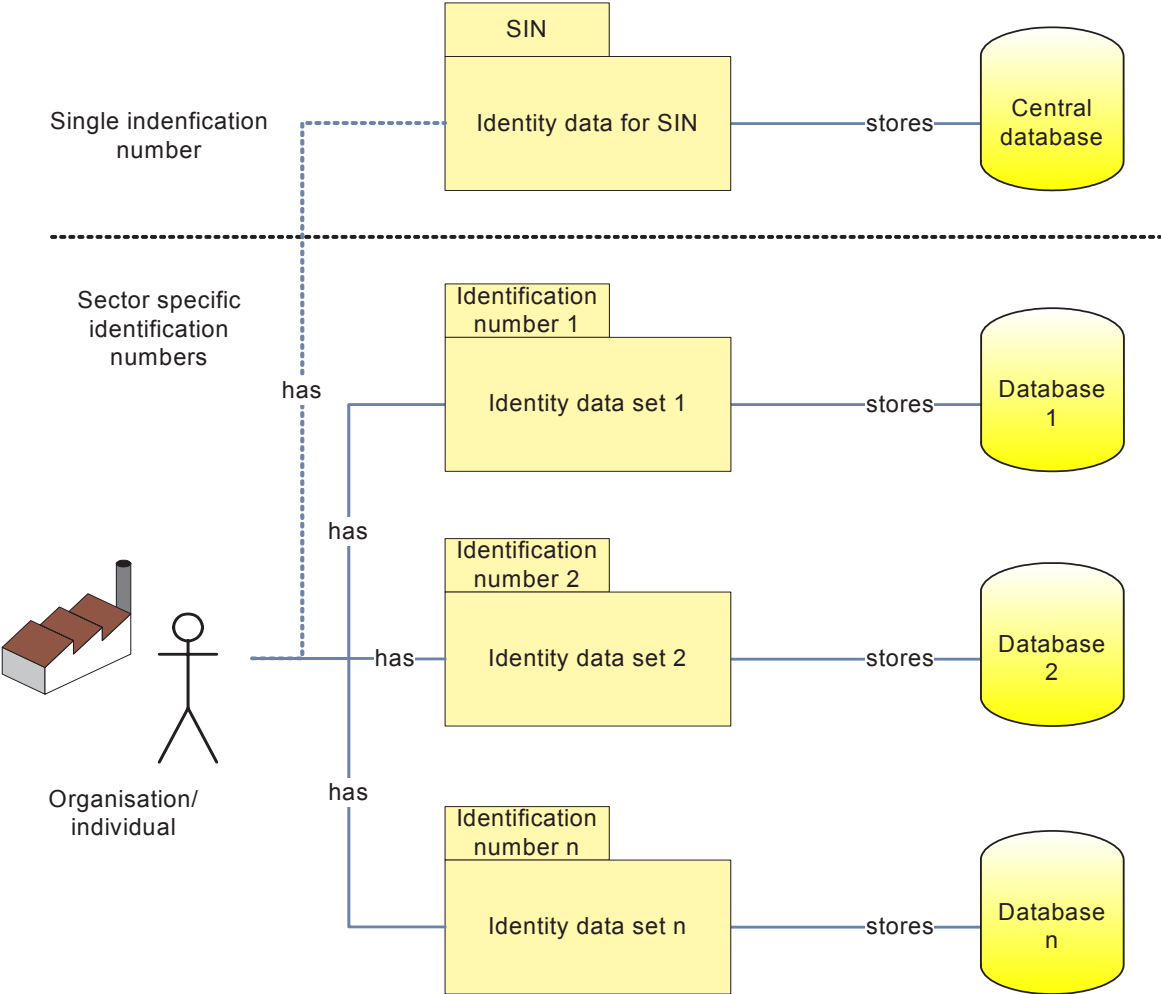


Figure 2: Independent systems for identification

In fact, figure 2 leads us to the notion of *sector specific ids*, which go in a certain sense beyond the mere concept of identifying an individual because they add very often certain specific, application oriented aspects to the above shown data set. The report shows that the more traditional and pragmatic systems do not differentiate precisely between sector and mere identifying oriented identity systems.

On the other hand, the more or less totally independent systems shown in figure 2 augment the “degree of privacy” to a certain extent, since data treated in sector x cannot be linked easily to personal data treated in sector y. From a more technical viewpoint, it is evident that such systems run possibly into the known problems of coherent data updates, multiplied communication needs and so on – short, interoperability becomes an issue.

Regarding the really single national identifier systems, figure 3 shows three potential scenarios two of which we found in the member states.

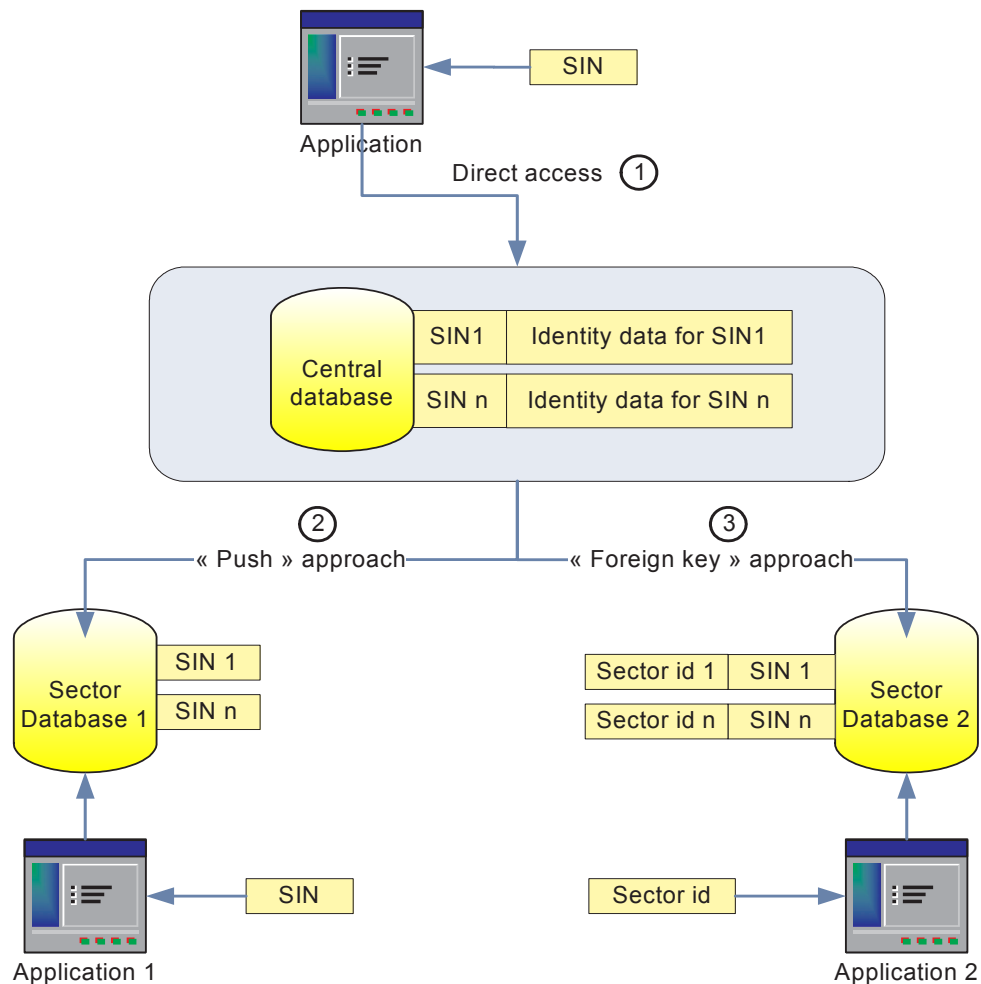


Figure 3: Central approaches to identity management

Common to all three scenarios in this figure is one central database with one central point of administration of the identity data record. Here, scenario 1 is rather hypothetical in assuming that there is only one database for all different sectors that is accessed online. Given the numerous different IT systems and registers in the public sector, this theoretic approach is not realisable – even from a technical point of view, let alone data protection concerns.

The scenarios 2 and 3 of figure 3 are more realistic and have been found for example in Luxembourg (2) and Malta (3).

In scenario 2, the identity data stored in a central database is propagated (pushed /pulled) to local, sector or administration specific databases that use the same SIN as key. Hence any update of the identity records can be forwarded to local databases as well.

In scenario 3, the sector specific registers are linked to the central database by storing the SIN as primary or foreign key⁴ in the corresponding databases, and maintaining local identifiers (and possible additional identifying data like for example a field for a post office box). Hence sector applications benefit from a central data management regarding for example their basic address data and so on.

⁴ This is kind of a « virtual » link, and not exactly the same concept as the referential integrity approach in IT databases, because there is usually no online link or constraint checking between the databases.

The notion of a real “single” identification number is certainly not justified when different independent systems of identifying individuals and organisations exist in one country. One could argue therefore that scenario 3 is not “unique” in this sense either. One should underpin although that, conceptually seen, this scenario comes much closer to a real single system than the system of independent sector-specific ids described in figure 2.

It is worthwhile mentioning that most of the national systems have certain particularities that are not taken into account in the simplistic schemes above. For example, the hybrid and technically advanced Austrian system must be further detailed in order to categorise it. In this context, it is important to know that it aims to combine the privacy provisioned by sector-specific ids with the “organisational convenience” that comes with a central, SIN system. The Netherlands have multiple copies of central data on a municipal level.

The general classification shown in figure 2 helps to understand these national particularities, and to classify the different “philosophies” existing.

2.2.2. Question I.3: Alternatives if there is no SIN

Question I.3 was reserved to the countries where there is currently no SIN (at least for natural persons), hence only relevant for Germany, Hungary, Ireland and the UK.

The detailed answers of those countries can be found in annexe B. In fact, the UK and Germany use sector specific numbers as a “replacement” for the missing SIN, and Ireland indicates the existence of a “personal public service number” used by most public services to identify natural persons. We have no further details on this concept, but Ireland has short-time plans to put in place a new system anyway (cf. next question)

For the special case of Hungary, see next question.

2.2.3. Question I.4: Plans to change the current situation

The majority of countries have indicated that there are plans to change the current situation regarding the identity management.

Although this might be surprising at first look, especially since there are only a few states that have not yet a SIN solution in place, not all changes concern the basic identity management infrastructure or the administrative management of identity data. Instead, many countries report plans to get underway electronic ID cards and comparable devices or concepts – hence deal with the already mentioned and shown in figure 1.

As regards the situation in those member states that have not yet a SIN solution for natural persons in place, three out of the four report that there are projects in this area:

- Ireland will put in place a SIN together with an identity management policy within the next six months
- the UK is running the “ID Card” and “Citizen Information Card” projects which also envisage the installation of a SIN for natural persons in this country
- Hungary reports that it will create in 2005 a “Central Internet Gateway” for the authentication of users of eGovernment transactional services based on name/password/email or electronic certificate identification. This solution does not

seem to be a literal SIN approach, but obviously shall aid to solve the authentication problem for eGovernment applications in the absence of such.

Amongst the bigger group of countries who have already a SIN in place, three different trends can be observed:

- Some countries report that there will be fundamental changes to the current system, meaning that there will be changes of the basic concepts. France for example reports the development of an “identity federation system”, and the Netherlands envisage the creation of a “Civil Service Number” as of 2006.
- Some countries focus on the authentication aspects of identity management, i.e. report plans to install electronic ID cards. This is the case for Bulgaria, Malta and Spain.
- A third group of countries is concerned about data protection aspects of their current SIN system. The Czech republic indicates that there are national discussions ongoing regarding current coding of birth date and sex in their SIN (in terms of the conformity with data protection as well as the extensive usage of the SIN in all sectors). Similar concerns exist in Lithuania, where especially the extensive usage of the national SIN is also subject to discussions, and sector specific IDs are proposed as alternative.

We can summarise that the majority of countries who do not have yet a SIN for natural persons is about to install it, a certain number of countries thinks about electronic authentication solutions, and some have concerns about their current system in terms of its data protection “compatibility”.

2.3. Technical aspects of the single identification number

Questions 5 and 6 asked about the technical construction of the SIN (for legal and natural persons) and the data linked to it.

2.3.1. Question II.5: Technical construction of the SIN

As already pointed out in the Belgian study, there are chiefly two approaches that have been chosen in the different states:

- Either the purely random construction of the SIN,
- or a construction that codes identifying data, usually like date of birth and sex – resulting in an identifier having some “*semantics*”.

After the Belgian presidency’s study from 2001, Austria has invented a new system that uses encryption algorithms to generate general and sector specific identifiers. These identifiers are clearly thought to be used by electronic procedures in the area of eGovernment solutions.

From a technical point of view, there is no significant difference between the random and the semantic scheme. It is self-evident that semantic numbers are easier to memorize and easier to use in totally paper-based or manually supported processes.

The Austrian example however shows that sophisticated approaches that are intended to be used in electronic processes might be more compliant with data protection concerns. In this

regard, one should notice that the Czech Republic reports (cf. answer to question I.4) that there are national discussions ongoing about the coding of birth date and sex in the SIN.

The detailed overview of the different systems can be found in the annex.

2.3.2. Question II.6: Data linked to the SIN

The situation that has been described already in the Belgian Presidency's report in 2001 has not changed significantly since then. Still, some countries (as for example Cyprus) link more than 20 different information entities to the SIN, and retain history data of at least some fields, e.g. address. Others restrict the amount of information to the minimum necessary to identify individuals, as for example Lithuania. Please see annexe B to have a detailed overview of the different data actually stored.

Summing, and regarding the aspect of data protection and data sharing, it seems clear to us that there are two different approaches concerning this detail of the SIN: Countries with traditional systems as Malta and Spain have a pragmatic view and relate sector specific data to the SIN where appropriate and utile. Others restrict the data to the mere identification purpose of it. From a technical point of view, the first approach is "simpler" in terms of central data holding, coherence of data and so on. It might be regarded nevertheless as being more complex to guarantee its compliance with data protection needs.

2.4. Organisational aspects of the SIN

In section III of the questionnaire, we were particularly interested in finding out how the member states manage the identity issue in terms of groups of persons that are actually covered by the process. Furthermore, we have evaluated who is responsible for the management of the (central) database and whether and how other registers may access the data (compare figure 3). Finally we wanted to know which documents comprise the SIN. We have focused our analysis on natural persons in this paragraph.

2.4.1. Person subgroups covered by the SIN (Q III.7)

At first glance, there is a common understanding that a SIN should identify the citizens of a country. Actually, when going into details, the question is somewhat more complex. In this context, it is not surprising that there have been further person subgroups that were mentioned in the answers. Summing up, we have been reported for example:

- Residents
- Persons born in the country
- Foreign workers
- Migrants, refugees
- Persons who are liable to tax affairs

Different restrictions and provisions apply for the groups, and different ways of managing and storing the IDs exist.

The fact that for example also migrant workers normally obtain a national SIN reflects the situation that there is not yet a trans-national ID that could be used for identifying non-citizens. Furthermore, the different detail handling and provisions that exist in terms of the identity management of non-citizen subgroups might hamper cross national data sharing.

2.4.2. Public authority responsible for management of SIN database (Q III.8)

In most cases, the national Ministries of Interior are responsible for the authorities that are in charge of the management of the SIN database. However, there are some exceptions to this rule. In Sweden, for instance, this role is taken by the “Swedish Tax Agency”, which is a government authority under the Ministry of Finance.

The operating authorities are either dedicated registers like Lithuania’s People Register, or technical bodies like the “Luxembourg State Centre for Informatics”.

There is the special case of the Netherlands where the municipalities run and maintain their own local databases (for the A-Nr., see country’s summary). These databases are networked and coordinated by an organisation called “Personal Documents Agency” – again under the Ministry of Interior.

Summing up, again, there are national particularities of the identity management system. As regards the responsible authorities, however, the differences seem to be limited.

2.4.3. Registers accessing the SIN data and documents comprising the SIN (Q III.9)

Regarding the connection to the central database, Lithuania for example has reported an exhaustive list of Registers that actually access the central database – in this case supported by a specific technical replication solution provided by a database manufacturer. A similar list is given by Denmark and Malta, but those countries just “use” the SIN in other Registers.

Cyprus uses the SIN as primary key in sector specific databases – compare figure 3. As regards legal persons, many countries have already installed online accessible public registers of the data.

Summing, most countries allow either direct access or distribute the SIN and the related data to other registers – which should not surprise, because the usage of the SIN in such registers follows the idea of a *single* identifier. The technical realisation of the access however differs a lot, and Austria has put in place a sophisticated end highly secured system that does not fit in this classification at all.

Please verify section 2.5 for all data protection related questions in this domain.

As regards the documents that comprise the SIN, there is a more or less common subset of such that normally includes identity cards and passports, and very often sector specific documents like social security or health system cards. Beyond this, some countries like Cyprus, Spain and Denmark for example, use the SIN as a multipurpose identifying characteristic on nearly all documents with personal related data. This reminds of the usage of employee numbers in companies, where a pragmatic and demand-driven view prevails.

2.5. Legal issues

The legal issues concerning personal data protection in general and an identification number in particular encompass multiple viewpoints that could not be tackled in an exhaustive way in this survey. Therefore, the questionnaire rather aimed to provide information that could help drawing a global picture of the situation in Europe. Thanks to the answers received from eighteen countries, this report can probably provide some meaningful information in this context.

Like above, the general summary of the legal issues follows the sequence of the questions in the questionnaire. For each question or each group of related questions, a global comment is proposed, which aims to highlight the most significant elements of the answers received.

2.5.1. Laws brought into force to comply with the directive 95/46/EC

The question 10 asked which laws were brought into force to comply with article 8.7 of the Directive 95/46/EC on Personal Data Protection. The article 8.7 specifically deals with the issue of SIN or more generally identifiers of general applications.

The answers allow several observations.

First of all, it must be noted that in all of the countries that have answered to the legal part of the questionnaire, some specific legislation exists to handle the Personal Data Protection issue. This result is not very surprising, however.

According to the answer received, it appears that at least five approaches have been chosen to organise the legal protection of identifiers.

- Some countries handle the identification number issue within the general legislation on Personal Data Protection without specific provisions. For instance, Cyprus has no specific provisions on the processing of a national identification number in his law of 2001 on Processing of Personal Data.
- Some countries handle the identification number issue within the general legislation on Personal Data Protection but with specific provisions. For example, the Danish Act on Processing of Personal Data includes some specific statements on the usage of civil registration numbers.
- Some countries, like Sweden, manage the identification number issue with a dedicated rule within the Personal Data Protection legislation but also add some specific rules that apply in some situations (e.g. national registration database ruled by a specific legislation).
- Some countries have not any single identification number for natural persons but only specific identification numbers that are ruled by specific legislations. In Germany, for instance, sector specific laws govern the social security number and the tax administration number.
- In addition, some countries also have a special legislation that organises a national register in which identification numbers are stored. Belgium, for instance, has established such rules in his Law of the 8th August 1983, and Denmark in his Act N° 426 of 31st May 2000.

2.5.2. Authority monitoring the application of Data Protection legislation

The question 11 aimed to identify the national authority that is responsible for monitoring the application of the legislation on data protection, in conformance to art. 28 of the Directive 95/46/EC.

The discussion of the results is quite limited as all countries have established a national authority, such as the ‘*Commission Nationale de l’Informatique et des Libertés*’ in France, or the ‘*Agencia Española de Protección de Datos*’ in Spain.

Nevertheless, the case of Germany is worth being specifically noted. Indeed, in this federal country, two levels of authorities have been created to monitor the application of the data protection legislation. The Federal Commissioner of Data Protection is responsible for data processed by public authorities at the federal level and the Land Commissioner for Data Protection is responsible for data processed by public authorities at the *Länder* level.

2.5.3. Processing of Personal Data: Obligation to notify the authority

Three questions (Q12a,b,c) were related to the obligation to notify the supervisory authority before carrying out any processing operation of personal data.

As regards the general notification requirement (Q12a), it is not sure whether the question has been understood in the same way by all responders. Indeed, the question was related to the exchange of data between administrations *making use of a SIN* but it seems that the answer of some countries refer to any exchange of data between administrations, independently of the usage of a SIN.

In most of the countries, a general notification to the supervisory is required before processing personal data. For instance, in Austria, as a matter of principle, each data application has to be notified to the Austrian data Processing Register.

Some countries answered with complementary information about the specific case of SIN processing. In these cases, the general approach seems to consider the SIN analogous to other personal data and therefore not to submit it to special rules for the obligation to notify the supervisory authority. For instance, in Denmark, no specific notification is required on the sole basis that the processing concerns civil registration numbers. Similarly, in Ireland, the notification requirement is not related to the processing of the SIN.

The question 12b concerned the presence of exemptions to the notification rule.

According to the answer received, only Denmark and Ireland offer no possibilities for exemptions. In all other countries, exemptions to the rule are possible. These exemptions fall into several categories:

- appointment of a personal data protection official (e.g. Luxembourg, Netherlands, Malta);
- specific data processing explicitly listed in legislation (e.g. Austria, Belgium, Sweden);
- processing of data with political, philosophical, religious or trade-union aims (e.g. Czech Republic, Lithuania);
- processing of data with national or public security concerns (e.g. France).

The question 12c asked whether the personal data processing is subject to prior checks (cf. art. 20 of the Directive).

Different attitudes may be encountered:

- In some countries, no prior check is required. This is the case, for instance, in Cyprus, Denmark, Ireland, and the United Kingdom.
- Other countries impose a prior check in some cases, depending on the nature of the data processing or on its context. The following examples illustrate this approach. In Lithuania, the supervisory authority, namely the State Data Protection Inspectorate, shall carry out prior check in specific situations such as the process of special categories of personal data (e.g. health care). In the same context, in Malta, prior checking is mandatory for all processing operations that involve risks of improper interference with the rights and freedoms of data subjects. In the Netherlands, prior checking is obligatory when the SIN is used for other purposes than described by law.
- Some countries also rely on the initiative of the supervisory authority. For instance, in the Czech Republic, if the Office for Personal Data Protection, after having been notified of a personal data processing, has a justified concern about the processing, it shall initiate proceedings at its own instigation.

2.5.4. Rights of the data subject

The Directive 95/46/EC guarantees several rights to the data subject (i.e. the person whose data is processed or recorded): an *information and notification right* (art. 10, 11), an *access right* (art. 12) and a *right to object* (art. 14). The question 13 related to how these rights are realised in the national legislations.

From a very general viewpoint, all these rights are granted in the national legislations of the countries having sent an answer to the questionnaire. It is useful, however, to discuss in detail each of these rights to point out some nuances in their implementation.

2.5.4.1. Information and notification right

In all countries, the data subject has an information and notification right. Nevertheless, the information that is communicated to the data subject, the time when it is communicated and the process of communication may vary.

The set of data that is notified to the data subject at least includes the purpose of the data process, as well as the name and address of the controller. In many cases, it is requested to communicate complementary data, such as the recipient or the categories of recipient of the data (e.g. Belgium, Cyprus), the rights of the data subject concerning the processing of his personal data (e.g. Belgium, Hungary), the mandatory or optional nature of the answer (e.g. Belgium), the consequences of the refusal to answer (e.g. Cyprus), the legal basis of the data processing (e.g. Hungary).

The answers have shown that some countries provide some exemptions to this right. The most usual exemptions are summarized in the (non-exhaustive) list below:

- processing of personal data obtained with the consent of the data subject (e.g. Czech Republic);

- personal data processing imposed by an act or a law (e.g. Czech Republic, Hungary);
- personal data processing performed for statistical, historical or scientific purposes (e.g. Czech Republic);
- personal data processing carried out for national security reasons (e.g. Cyprus);
- personal data processing in the context of detection of criminal offences, or related investigation (e.g. Cyprus);
- processing of lawfully published personal data (e.g. Czech Republic).

2.5.4.2. Access right

This right is given to the data subject in all countries having answered to the question.

The data subject has usually access to the following information:

- the confirmation that some data concerning him/her are or are not processed,
- the processed data,
- the available purpose of the use of data, and
- the recipients of the data.

In some countries, the data subject has access to complementary information. For instance, in Austria, he or she has access to the legal basis of the processing, and this in an intelligible form. In Cyprus, there is a right to access to the progress of the processing. In Sweden, access to where the data has been collected is granted.

In order to have access to this information, the data subject has normally to prove his or her identity. Moreover, some countries demand the request (e.g. Austria, Poland) or the answer (e.g. Malta, Poland, Sweden) to be made in writing.

Included with the access right, the data subject is given the right to obtain the correction of any incorrect personal data that concerns him/her. Some countries mention that the correction must be offered free of charge to the data subject (e.g. Belgium).

Finally, it must be noted that some countries provide exceptions to the access right as the two following examples illustrate: Ireland reports some exceptions but they are said to preserve an individual right to access information. In Sweden, access must not be provided in some exceptional situations, where the Secrecy Act prescribes that information may not be disclosed to the data subject.

2.5.4.3. Right to object

In all the countries that have answered the questionnaire, the data subject is given a right to object.

As mentioned in the Directive, the right to object is normally provided in two situations:

- when the data subject has serious and legitimate reasons to object the processing of some data;

- when the personal data are collected for direct marketing purpose.

2.5.4.4. Implementation of the access to data

The question 13b targeted the implementation of the access right of the data subject. In particular, the question asked whether online access were available.

First of all, it must be mentioned that the access mode to the personal data is normally not specified by law. The type of access given to the data subject depends on the specific context. Several approaches may be identified from the cases reported in the answers.

- In Belgium, due to the existence of an electronic identity card, online access is allowed and authentication is achieved via the identification certificate stored on the electronic identity card. Any titular of an electronic identity card may also ask which data is stored on the card.
- Some countries offer online access but only for some registers (e.g. Bulgaria, Denmark, France, Spain).
- In the United-Kingdom, since January 2005, the information may be sent by e-mail to the person making the request.
- In the Netherlands, individuals in general do not have online access to their data.
- In Germany, the architecture and the concepts for access to electronic healthcare records are under development.

Finally, independent from the position of each country, the access to personal data usually requires from the data subject to prove his or her identity, either electronically (e.g. Belgium, Denmark) or in writing (e.g. Austria, Sweden).

2.5.5. Data sharing between administrations

The set of sub-questions grouped under question 14 related to the legal framework that rules the transfer, sharing, interconnection and exchange of personal data between public agencies or administrative authorities *by using a SIN*.

Like for question 12 a), it seems that the questions have been understood in two ways. Some countries considered the general case of data sharing between administrations and others focused on the specific case of data sharing between administrations *by using a SIN*.

The first question (Q14 a) asked whether those operations have to be authorised explicitly by a specific law or any other provision, in particular if the public interest pursued and the purpose for which the data is intended by the different administration are different.

For the *general* data sharing between administrations, it appears that, in most of the cases, the processing has to be authorised by specific laws (e.g. Hungary, Netherlands, Sweden). Some other approaches may however be encountered. In Belgium, for instance, the authorisation is given by the supervisory authority. In Cyprus, the provisions of the general Data Protection Law cover the cases related to this issue.

For the data sharing between administrations *by using a SIN*, the collected answers allow pointing out that many countries have no specific authorisation or provision that would apply

in this specific case. For instance, Austria mentions that ‘regardless of the constitutional principle that every usage of data by a public authority requires the legal form of an act, no additional authorisation is needed due to the use of new identifiers’. Nevertheless, some exceptions are reported. In Ireland, for instance, the sharing of data using a single identifier has to be allowed by law.

The second question (Q14b) asked if the supervisory authority has to be asked for comment before giving such an authorisation.

According to the answers received, several attitudes may be distinguished.

- Some countries, such as Lithuania or the Netherlands, do not require the comment of the supervisory authority.
- Some countries mention that the supervisory authority has to be consulted in some specific circumstances. For instance, in Malta, comments are required only in cases where there is a risk of improper interference with the rights and freedoms of the individuals.
- Some countries, like Ireland or Spain, do not require the supervisory authority to be asked for comments but in practice, there is often some consultation.
- Some countries, like Hungary or Sweden, remind that the supervisory authority is consulted during the legislative process.
- Some countries, like Cyprus, require the supervisory authority to be involved.

The third question (Q. 14c)) dealt with data sharing at the international level and asked whether it is submitted to specific provisions.

First of all, it must be reminded that transfers within the EU should be considered in the same way than national transfers. The question gains thus greater interest in the case of data sharing with non-EU countries.

Most of the countries impose some specific and possibly cumulative provisions, such as:

- the transfer to foreign country is allowed only if this country assures an adequate level of personal data protection (e.g. Belgium, Hungary, Malta);
- the transfer demands a specific legal basis to take place (e.g. Denmark);
- the transfer is permitted if the data subject has provided his consent (e.g. Hungary, Lithuania);
- the transfer is necessary for the prevention or investigation of criminal offences (e.g. Lithuania);
- the transfer is necessary for the conclusion or performance of a contract with specific requirements (e.g. Lithuania).

2.5.6. Shared databases

The question 15 investigated the issue of shared databases, in particular when these databases are deployed by public authorities and agencies and when the data stored includes at the same time common entities recorded or accessed by all organisations and entities restricted to the organisation(s) for which these entities are relevant.

The responding countries have adopted two main kinds of attitude concerning this point.

- On the one hand, most of the countries allow the presence of shared databases, but only in some specific circumstances and under strict conditions. First of all, the operations relative to shared database must obviously meet the principles stated in the Personal Data Protection legislation. In addition, some countries impose some specific and sometimes cumulative conditions, such as:
 - obtaining prior checking and authorisation by the supervisory authority (e.g. Austria, Belgium, Luxembourg);
 - being authorised by a specific law (e.g. Denmark, Malta);
 - being kept up-to-date and not being considered as reference data source (e.g. Belgium);
 - taking appropriate measures to ensure that the admissibility of individual access can be monitored at all time (e.g. Germany);
 - appointing a suitable operator for the shared database (e.g. Austria).
- On the other hand, some countries, like the Czech Republic or Hungary, do not allow shared databases. Yet, some mechanisms to exchange data, in particular for synchronizing purposes, are permitted.

2.5.7. Allowed uses of the Single Identification Number

Question 16 grouped three questions referring to the cases where the use of a SIN is allowed.

It must be noted that, in this summary, only SIN associated to natural persons will be considered. Indeed, most of the answers focus on this case of use while a few countries also provided information about SIN for legal persons.

The first case that was under examination (Q16a) concerns the use of the SIN by private bodies for their internal needs. The answers show that very divergent attitudes can be encountered.

- Some countries, like France, Belgium or Lithuania, prohibit the use of the SIN in this case.
- Some countries, allow the use of the SIN but enforce strict conditions, such as:
 - explicit consent of the data subject (e.g. Sweden, Denmark);
 - use follows from law or regulation (e.g. Sweden, Denmark);
 - processing is carried out for scientific or statistical purposes (e.g. Denmark).

- Some countries, such as Spain and Bulgaria, allow using the SIN in this case.
- The case of Austria, which has one of the most advanced systems for managing identification numbers, is worth being explicitly discussed. This country allows the use of sector specific identification number (ssPIN) or private sector specific PIN (pssPIN) derived mathematically from a source PIN. It is required, however, that a given person has different ssPIN / pssPIN within the databases of different private bodies.

The second case that has been studied (Q16b) concerns the use of the SIN in contacts between private bodies and citizens. In fact, nearly all countries regulate this situation in the same way than the preceding one (use of the SIN by private bodies for their internal use).

The third case (Q16c) relates to the use of the SIN in contacts between private bodies and public administration.

Several countries permit the use of the SIN for such contacts (e.g. Bulgaria, Lithuania). In some cases, this type of use is allowed while the two preceding are prohibited (e.g. Belgium).

The other countries limit the circumstances in which the use of the SIN is allowed (e.g. in France where the use is limited to contacts with social security organisations) or add conditions similar to those required for the two previous cases (e.g. explicit consent of the data subject).

2.5.8. Present and future of the national situation

The last question (Q17) was really an open one. The contact person was asked to assess the current legal situation in his or her country in terms of any legal or regulative hindrances concerning the sharing of identity data. We also asked to identify some drivers, legal or others, to increase the sharing of identity data. Finally, we asked about short- or mid-term national projects relative to this issue.

The auto-assessment of the domestic situation by each country brings significant insights for the understanding of the whole picture.

Some respondents judge that the system currently in use in their country is satisfying and they do not mention any serious complaint against it. For instance, in the case of Germany, the reasons for existing hindrances are said to be justified and the respondent emphasises that there is no need for change. Similarly, the respondent from France declares that the law on the personal data protection may be considered as a hindrance but it is yet necessary. In Spain, the personal data protection is considered by the respondent as well developed and as including the required security measures. In Cyprus, the sharing of identity data, when needed, is said to be resolved in a satisfying manner by specific licences granted by the supervisory authority.

Other respondents identify some possible directions for improving their national system. The respondent from Lithuania mentions that the system of unique personal identification should be amended either by providing a system of sector based identification or by limiting the justified processing of the PIN by law. Additionally, he declares that the number of legal persons indicated in the Law on Legal Protection of Personal Data should be reduced to the necessary cases. In Sweden, the respondent tells that the regulation lacks an overarching information resource perspective, which has resulted in fragmented legislation and different technical and administrative solutions in different sectors.

The respondents were also invited to specify some drivers that support the sharing of identity data. Several specific drivers have been mentioned:

- better service to the citizen by not asking him many times his identification data (cf. Belgium);
- quest for efficiency and better services to citizens (cf. Sweden);
- provision of personalised public services (cf. United Kingdom);
- reduction of the risk of mistaken identity, accurate identification of persons (cf. Cyprus, Lithuania);
- financial drivers (cf. Sweden);
- new law for electronic handling of public administration processes (cf. Hungary);
- law enforcement purposes (cf. Cyprus);
- security issues (cf. Cyprus, United Kingdom).

From a more general viewpoint, some respondents report that the sharing of identity data is part of a political statement (cf. Belgium) or results from an eGovernment initiative (cf. Ireland).

Finally, the very last question investigated the future and aimed to identify some projects that might be planned in the domain of identity data sharing.

- Austria will continue to develop its advanced system. The sharing of identity data will most probably not be necessary in the future, thanks to the usage of a citizen card, which will provide authorised and standardised identification data legally approved.
- Belgium supports the build-up of an identity data store at European level.
- Germany currently develops an architecture and the concepts for access to electronic healthcare records and other data managed by the use of an electronic health card.
- In Hungary, executive decrees of the new law for public administration processes are under preparation. They will define the details of the identity sharing model of the public administration.
- In Lithuania, the supervisory authority prepares a modification of the Law on Legal Protection of Personal Data limiting the scope of the subjects who have the right to use the personal identification number.
- The Netherlands have launched a collection of projects that intend to realize ‘basic registers’ concerning six different registers. Moreover, a Civil Servant Number is foreseen to be introduced in 2006.
- In Poland, some reflections are currently undertaken in order to modernize the current PESEL system handling the identification numbers. Among others, a new architecture for simplifying the several registration levels is being studied. Another meaningful example of the ongoing reflection concerns the geographical extension of the network underlying the PESEL system, in order to reach every municipality.

- In Sweden, some discussions are going on regarding increased possibilities for exchange of data between authorities that handles allowances (e.g. social insurance, social welfare) in order to avoid fraud situations. In addition, a proposal for a new Secrecy Act contains some rules that would open up for increased possibilities to exchange data.

To conclude, it must be noted that some countries explicitly emphasized the fact that the protection of personal data must be continuously assessed compared to the efficiency and quality of public services. Some contradictory requirements must always be balanced.

3. Conclusions

Before summing up the results of the present study, two principal limitations regarding its scope and its significance have to be noted. First, as a *horizontal* restriction, not all of the member states and candidate countries have answered to the questionnaire. Hence, all conclusions drawn are –strictly spoken– just valid for “the member states and candidate countries that have answered to the questionnaire”. For the reason of readability, we simply speak of Europe or “all countries”. Second, as a *vertical* restriction, the study can only highlight its subjects, because identity management and especially data protection and data sharing are very complex and emerging topics, and because the scope of the answers has differed – depending on the question and the country.

Nevertheless, the results obtained and the comparison with the study of the Belgian presidency of 2001 lead to some interesting conclusions that might help to gain a sound first insight into the treated issues.

As a further general remark, it is worthwhile to mention that there is a clear difference between identifiers for natural and legal persons. For natural persons, there are normally concerns and most often also formal rules in order to protect its usage – even if the degree of attentiveness in this area differs. For legal persons, most countries have not indicated such concerns. It seems that IDs for legal persons are handled pragmatically, and that most countries regard their identification as a technical issue which has no or just a “slight” link to data protection issues. This observation allows us to focus on natural persons in this section hereafter.

As a last important general remark, we must underpin that there is no “optimal” solution for the identification issue in eGovernment. National culture, legal aspects, technical feasibility, costs and much more factors have to be taken into account when installing or deploying such solutions. Furthermore, a couple of countries pointed out explicitly that legal “obstacles” are *wanted* obstacles. The objective of the Directive 95/46/EC, for instance, was not to ease data sharing – it provided regulations in terms of the “protection of individuals with regard to the processing of personal data”. This report is neutral in terms of the quality of national approaches – it strives to describe the differences and to raise the awareness of them.

After these introducing, more general remarks, we focus now on the mere existence of a SIN in Europe. The report shows a tendency towards the acceptance of such an identification concept. Since the Belgian study from 2001, three countries have either realised former plans to introduce a SIN for natural persons (Austria) or such plans do exist meanwhile and are likely to be realised in the near future (Ireland and the United Kingdom). Germany is now the only country of the 15 states that have already been member in the Union in 2001 that has no and does not want to install a single identifier. Hungary, a new member state, shares this attitude.

Regarding the legal aspect that has also been investigated, all countries have brought in force national laws and regulations that are conform to the Directive 95/46/EC.

Hence, on a very general level, one might assume that the framework for the essential question of Pan-European data sharing of person-related data can be regarded as kind of a “piece-of-cake”-problem: There is a SIN nearly everywhere, and all members refer to the same directive for regulating data protection.

Of course, this would be a rather naïve conclusion, and this study would not have been necessary to confirm this.

The problem starts with the notion of the SIN itself. As already pointed out in the Belgian study, the identifier is not “really” single in most of the countries that have indicated that they have such a SIN. As a matter of fact, the majority of the respondents have reported the existence of further identification systems in their countries. Sometimes, these numbers are totally independent from each other and/or the “single” identifier; sometimes there are common keys or other mechanisms of synchronisation between these sector specific numbers and the general, central identifier. The degree of centralism depends on technical or historical conditions. Technically advanced systems like the Austrian one realise a hybrid approach that combines sector specific and central IDs in a more specialised form. Here, Austria and e.g. Belgium benefit from the fact that their national systems are new and could be designed according to recent eGovernment and data protection needs and insights.

For most of the countries, however, the fact that parallel and sector specific ids exist is a clear obstacle when sharing data already on a domestic level – and might cause even more trouble when such an exchange happens in a cross-border administrative process.

Besides the denomination problem, the construction of the identifier is based chiefly on two different philosophies. The first and bigger group of countries use a semantic approach in terms of coding usually the birth date, the sex and seldom further information. The second group uses random numbers, sometimes with data protection concerns as reason for this. Again, these diverging attitudes might cause problems when international data exchange is envisaged.

Further remarkable discrepancy exists in terms of the handling of the SIN. To highlight just a few of them:

- Some countries use a central register for the SIN that stores a lot of sector specific data and hence go far beyond the mere identification objective of the number. Other countries are rather minimalist concerning the data stored.
- The person subgroups obtaining a SIN are not identical. There are specific rules resulting probably from national particularities (like, for example, a great number of cross-border commuters) and traditions, even if the number is normally given to at least “all citizens”.
- The documents that comprise identifying numbers differ from country to country. Most of the countries use the number on identity cards and passports; a few countries have reported an extreme wide and daily use on all documents that include personal data in public and private affairs. A couple of countries do already comprise the number on electronic identification cards.
- The kind of legislative framework set up to rule the use of identification numbers varies. Some countries handle this issue within the general legislation on data protection, with or without specific provisions. Others regulate the identification number issue with (sector) specific laws. Finally, in some countries, a dedicated law organises a national register, which stores the identification numbers.
- The supervisory authority may play various roles concerning the protection of personal data. Depending on the country concerned, the situations where the supervisory authority is notified, consulted for comments, or asked for authorisation vary significantly.
- The three basic rights mentioned in the directive (information and notification right, access right, right to object) are granted to the individuals with some variations. The

following examples illustrate this diversity: The composition of the data set notified to the data subject, the exemptions to the information and notification rights, or the data set to which the data subject has access, are different from country to country.

To sum up all this difference, and as a general conclusion: The reality regarding single identification numbers and the related data protection legislation and provisions in Europe is heterogeneous. This heterogeneity results obviously from the different national legal, political and historical framework on the one hand, and the actual chosen solutions for identity management on the other hand. Despite this heterogeneity, the vast majority of countries is concerned about data protection related issues when dealing with identification numbers.

Even if in most cases there has not been a formal risk-benefit analysis of possible identification management solutions, since most countries have been using such approaches since decades, one could nevertheless propose a explanatory model (cf. figure 4) that

- relates the identification management topic to the data sharing and data protection area
- shows that different drivers (or possible benefits) exist with currently throw up and push the question of identity management
- clarifies that normally the possible solutions bear risks – among which the question of the installation of a *single* identifier is perhaps the most basic one to answer.

As we have seen, most of the countries affirm the installation of a SIN. Nevertheless, the countries who decide not to put in place such a system must and do use different mechanisms for identification. The evaluation criteria used depend extremely on national particularities and politics.

Irrespective from basic decision whether to install a SIN or not, the concrete realisation of the national solution consists not only of the implementation of a mere number, but of a complete package of different measures and procedures. Taking a formal approach, this package can be seen as a *triplet of organisational, technical and legal measures and provisions*.

This report shows the high discrepancy of these national triplets. It is evident that this hampers cross-border data sharing. But, as already pointed out above, this is –technically seen- a neutral statement, since this hindrance might be volitional from a political point of view.

Contrariwise, the divergence of the triplets does not totally exclude cross-border data sharing. The report has shown that there are yet a lot of similarities, for instance the tendency to affirm the necessity of a SIN or the Directive 95/46/EC as common base for national data protection legislation.

Any eGovernment solution that realises Pan-European data sharing should nevertheless scrutinize the concerned national triplets in its analysis phase and strive to find compatible solutions.

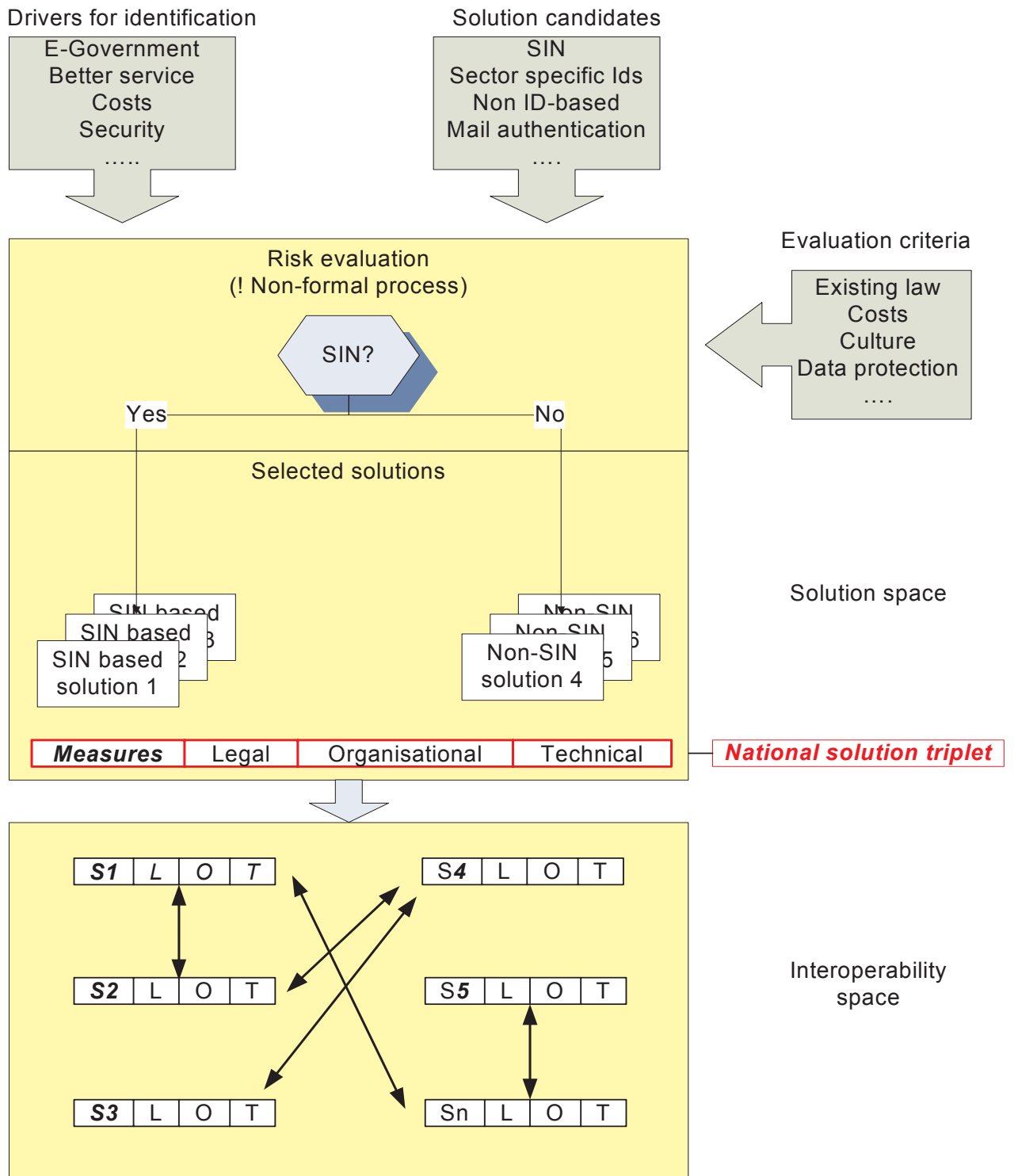


Figure 4 : Identity management and data sharing

A. Annexe : Country Summaries

A.1. Austria

Has taken part in 2001 Belgium study?	Yes
Significant change (SIN part)	Yes

Single Id. for natural persons	Yes
Single Id. for legal persons	Yes

National Legislation related to Directive 95/46/EC (in particular art. 8.7)	Austrian E-Government Act, Federal Law Gazette part I no. 10/2004 (E-Gov-Act) Data Protection Act (Datenschutzgesetz DSG) 2000 General Social Insurance Act, Federal Law Gazette no. 189/1955 (GSI-Act)
Supervisory Authority	Austrian Data Protection Commission

Some key features	<ul style="list-style-type: none">❖ One of the most technically advanced systems for managing the identification number issue, takes into account high data protection and technical needs at the same time❖ Use of sector specific id. numbers derived from a source id. number❖ Citizen card planned storing id. data
-------------------	---

A.2. Belgium

Has taken part in 2001 Belgium study?	Yes
Significant change (SIN part)	Yes

Single Id. for natural persons	Yes
Single Id. for legal persons	Yes

National Legislation related to Directive 95/46/EC (in particular art. 8.7)	Law of 8 th August 1983 organising a National Register for Natural Persons Law on the Protection of Private Life of 8 th December 1992
Supervisory Authority	<i>Commission de la Protection de la Vie Privée / Commissie voor de bescherming van persoonlijke levensfeer</i>

Some key features	<ul style="list-style-type: none"> ❖ Electronic identity card in use ❖ Political statement that each federal administration should not ask identification data to citizens or companies if those data are already available in other federal administrations
-------------------	--

A.3. Bulgaria

Has taken part in 2001 Belgium study?	No
Significant change (SIN part)	N/A

Single Id. for natural persons	Yes
Single Id. for legal persons	Yes

National Legislation related to Directive 95/46/EC (in particular art. 8.7)	Law on Protection of Personal Data, published 4 th January 2002.
Supervisory Authority	Commission for Personal Data Protection

Some key features	❖ e-Service on-line to access personal data, with the use of e-certificate
-------------------	--

A.4. Cyprus

Has taken part in 2001 Belgium study?	No
Significant change (SIN part)	N/A

Single Id. for natural persons	Yes
Single Id. for legal persons	Yes

National Legislation related to Directive 95/46/EC (in particular art. 8.7)	Processing of Personal Data (Protection of Individuals) Law of 2001 (138/2001), entered in force in November 2001
Supervisory Authority	Commissioner for Personal Data Protection

Some key features	<ul style="list-style-type: none"> ❖ Large amount of data linked to the identification number ❖ National SIN is primary key in almost all government IT systems
-------------------	---

A.5. Czech republic

Has taken part in 2001 Belgium study?	No
Significant change (SIN part)	N/A

Single Id. for natural persons	Yes
Single Id. for legal persons	Yes

National Legislation related to Directive 95/46/EC (in particular art. 8.7)	Act no. 101/2000 Col. on the Protection of Personal Data, 4 th April 2000
Supervisory Authority	Office for Personal Data Protection

Some key features	❖ Current discussions about coding of birth date and sex in SIN as well as about extensive usage of it in private and public institutions.
-------------------	--

A.6. Denmark

Has taken part in 2001 Belgium study?	Yes
Significant change (SIN part)	No

Single Id. for natural persons	Yes
Single Id. for legal persons	Yes

National Legislation related to Directive 95/46/EC (in particular art. 8.7)	Danish Act on Processing of Personal Data (Act no. 429 of 31 st May 2000)
Supervisory Authority	Danish Data Protection Agency

Some key features	❖ Strong concerns about individual's legal rights and protection of personal data
-------------------	---

A.7. France

Has taken part in 2001 Belgium study?	Yes
Significant change (SIN part)	No

Single Id. for natural persons	Yes
Single Id. for legal persons	Yes

National Legislation related to Directive 95/46/EC (in particular art. 8.7)	Loi du 6 août 2004 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel
Supervisory Authority	<i>Commission Nationale de l'Informatique et des Libertés</i>

Some key features	❖ Evaluates an “identity federation system” for E-Government applications
-------------------	---

A.8. Germany

Has taken part in 2001 Belgium study?	Yes
Significant change (SIN part)	No

Single Id. for natural persons	No
Single Id. for legal persons	No

National Legislation related to Directive 95/46/EC (in particular art. 8.7)	Federal Data Protection Act (Bundesdatenschutzgesetz, BDSG, in the version published on 14 th January 2003, Federal Law Gazette I 66)
Supervisory Authority	Federal Commissioner for Data Protection Land Commissioners for Data Protection

Some key features	<ul style="list-style-type: none"> ❖ Use of Sector Specific Id. Numbers, ❖ Multi-level supervisory authority ❖ Does not plan to install SIN for natural persons because of data protection concerns
-------------------	--

A.9. Hungary

Has taken part in 2001 Belgium study?	No
Significant change (SIN part)	N/A

Single Id. for natural persons	No
Single Id. for legal persons	Yes

National Legislation related to Directive 95/46/EC (in particular art. 8.7)	Act on Protection of Personal Data and Disclosure of Data of Public Interest, 1992 Special law for the privacy harmonised completely with the Directive 95/46/EC
Supervisory Authority	Data Protection and Freedom of Information Commissioner of the Hungarian Parliament

Some key features	<ul style="list-style-type: none"> ❖ New legislation under preparation to rule, among others, the identification data sharing ❖ Is about to install a central gateway for authentication and identification of persons who want to use E-Government applications. System not based on a SIN.
-------------------	--

A.10.Ireland

Has taken part in 2001 Belgium study?	Yes
Significant change (SIN part)	Yes

Single Id. for natural persons	No
Single Id. for legal persons	No, but planned

National Legislation related to Directive 95/46/EC (in particular art. 8.7)	Data Protection (Amendment) Act 2003 Social Welfare Acts (1998-2003)
Supervisory Authority	Data Protection Commissioner

Some key features	❖ Is about to install a SIN, driven by E-Government needs
-------------------	---

A.11. Italy

Has taken part in 2001 Belgium study?	Yes
Significant change (SIN part)	No

Single Id. for natural persons	Yes
Single Id. for legal persons	Yes

National Legislation related to Directive 95/46/EC (in particular art. 8.7)	Data Protection Law (Law N. 675/1996), amended in 2001
Supervisory Authority	No answer

Some key features	<ul style="list-style-type: none">❖ Electronic ID card in use❖ SIN for natural persons changes when name changes
-------------------	---

A.12.Lithuania

Has taken part in 2001 Belgium study?	No
Significant change (SIN part)	N/A

Single Id. for natural persons	Yes
Single Id. for legal persons	Yes

National Legislation related to Directive 95/46/EC (in particular art. 8.7)	Law on Legal Protection of Personal Data Law on Population Register, Regulations of Population Register.
Supervisory Authority	State Data Protection Inspectorate

Some key features	❖ Trend to limit more strictly the use of identification number
-------------------	---

A.13.Luxembourg

Has taken part in 2001 Belgium study?	Yes
Significant change (SIN part)	No

Single Id. for natural persons	Yes
Single Id. for legal persons	Yes

National Legislation related to Directive 95/46/EC (in particular art. 8.7)	Law of 30 th March 1979 organising the digital identification of physical and legal persons Data Protection Act of 2 nd August 2002
Supervisory Authority	<i>Commission Nationale pour la Protection des Données</i>

Some key features	❖ Wide usage of SIN and the corresponding infrastructure in public sector
-------------------	---

A.14.Malta

Has taken part in 2001 Belgium study?	No
Significant change (SIN part)	N/A

Single Id. for natural persons	Yes
Single Id. for legal persons	Yes

National Legislation related to Directive 95/46/EC (in particular art. 8.7)	Data Protection Act 2001 enacted on 14 th December 2001
Supervisory Authority	Commissioner for Data Protection

Some key features	<ul style="list-style-type: none">• Electronic ID-Card will probably have an impact or change the current SIN system
-------------------	--

A.15.Netherlands

Has taken part in 2001 Belgium study?	Yes
Significant change (SIN part)	No

Single Id. for natural persons	Yes
Single Id. for legal persons	Yes

National Legislation related to Directive 95/46/EC (in particular art. 8.7)	Personal Data Protection Act of 6 th July 2000
Supervisory Authority	Dutch Data Protection Authority (<i>Het College Bescherming Persoonsgegevens</i>)

Some key features	❖ New system of SIN (“Civil Service Number”) as of 2006
-------------------	---

A.16.Poland

Has taken part in 2001 Belgium study?	No
Significant change (SIN part)	N/a

Single Id. for natural persons	Yes
Single Id. for legal persons	Yes

National Legislation related to Directive 95/46/EC (in particular art. 8.7)	Law on the census and identity cards (voted 10.4.1974 with later changes, published in the Polish Official Journal No 2000.87.960)
Supervisory Authority	

Some key features	<ul style="list-style-type: none">❖ Modernization of the current system for handling identification numbers is foreseen❖ High attention paid to the conformity with EU standards for the new system
-------------------	--

A.17. Spain

Has taken part in 2001 Belgium study?	Yes
Significant change (SIN part)	No

Single Id. for natural persons	Yes
Single Id. for legal persons	Yes

National Legislation related to Directive 95/46/EC (in particular art. 8.7)	Law 15/99 on the Protection of Personal Data Electronic DNI regulated in the Law 59/2003 on electronic signature
Supervisory Authority	<i>Agencia Española de Protección de Datos</i>

Some key features	❖ Pragmatic use of SIN, appears on nearly every person-related document
-------------------	---

A.18.Sweden

Has taken part in 2001 Belgium study?	Yes
Significant change (SIN part)	No

Single Id. for natural persons	Yes
Single Id. for legal persons	Yes

National Legislation related to Directive 95/46/EC (in particular art. 8.7)	Personal Data Act (SFS 1998:204) entered into force 24 th October 1998
Supervisory Authority	Data Inspection Board

Some key features	<ul style="list-style-type: none">❖ Efficiency and better services to citizens and businesses❖ Initiatives to better exploit the potential of data sharing on the field: fight against fraud concerning allowances, crime prevention
-------------------	---

A.19. United Kingdom

Has taken part in 2001 Belgium study?	Yes
Significant change (SIN part)	Yes

Single Id. for natural persons	Planned
Single Id. for legal persons	No, not planned

National Legislation related to Directive 95/46/EC (in particular art. 8.7)	Data Protection Act 1998
Supervisory Authority	Information Commissioner

Some key features	❖ Id card related projects ongoing envisaging installation of SIN
-------------------	---

B. Annexe: Synoptical tables

The following tables will give a synoptical overview of the responses to the questionnaire. Please note that the answers have been somewhat edited and/or shortened in order to achieve a maximum level of readability and comparability of the results.

Please apologize that because of the different original format of the tables, the page numbering of the report could not be continued in annexe B.

Question I.2

Does your country use Specific id numbers in different sectors of the public administration?

Country	Natural Persons	Legal persons
Austria	Tax number, social security number, universities, others independent systems	no
Belgium	SIN used in all sectors after authorisation by National Register Tax number still used	SIN used after authorisation by National Register
Bulgaria	no	yes
Cyprus	Social security, national health system, passports, electoral cards have own numbers, but linked to SIN. Tax number, driver license number and others derived from SIN.	VAT, taxation numbers, but linked to SIN
Czech republic	Social security, others	no
Denmark	Social security, national health system, passports, electoral cards have own numbers, tax number, driver license number and others	Old numbering systems still in use, but being replaced more and more by SIN
France	yes	yes
Germany	-Pension insurance number, health insurance number, Tax number as of 2007	-Id for the social security system -ID for tax system as of 2007
Hungary	yes	yes
Ireland	yes (majority of public service sectors use "Personal public service number")	-tax number, company registration number, others
Italy	yes	yes
Lithuania	social security number	no
Luxembourg	no	no
Malta	yes	yes
Netherlands	social fiscal number, administration-number (a-nr), special education number	trade register number, fiscal number
Poland	Taxation number, but linked to SIN	Taxation numbers, but linked to SIN
Spain	yes	yes
Sweden	no	no
United Kingdom	national insurance number	no

Question I.3*When there is no SIN: alternatives?*

Country	Description
Austria	n/a
Belgium	n/a
Bulgaria	n/a
Cyprus	n/a
Czech republic	n/a
Denmark	n/a
France	n/a
Germany	see I.2
Hungary	natural persons: no, legal persons: yes
Ireland	"Personal Public Service Number" used by most public service agencies to identify natural persons
Italy	n/a
Lithuania	n/a
Luxembourg	n/a
Malta	n/a
Netherlands	n/a
Poland	n/a
Spain	n/a
Sweden	n/a
United Kingdom	"National Insurance Number" (NINO)

Question I.4 *Are there any plans to change the current situation?*

Country	Description
Austria	no
Belgium	no
Bulgaria	Introduction of Identity Cards with digital certificates is planned
Cyprus	no
Czech republic	-Discussions ongoing regarding current coding of birth date and sex in SIN (conformity with data protection) -Current extensive usage in private/public institutions is also discussed
Denmark	no
France	Identity federation model is being developed
Germany	no
Hungary	Central Internet Gateway for authentication of users of E-Gov transactional services based on name/password/email or electronic certificate will be put in place 2005. Unclear if this is based on a SIN-like system. (with propagation of information to further administrations and wide usage)
Ireland	Identity management policy for individuals being developed over the next six months. SIN to be used by all public service agencies
Italy	no
Lithuania	Wide use of SIN in being discussed (especially in the private sector). Proposals: sector specific numbers, limit number of the subjects allowed to use the SIN, encryption
Luxembourg	no
Malta	Use of electronic identification in E-Government will change system, possible use of Smart Card in the future
Netherlands	SIN is being developed ("Civil Servant Number"), installation 1/1/2006, use will be compulsory in G2C and G2G communication. No decision yet on the data linked to the number.
Poland	The SIN (DNI) will be used as eDNI also on electronic ID cards. These cards will store electronic signature, biometric data and other administrative data. The launch of the project is postponed to next year
Spain	The SIN (DNI) will be used as eDNI also on electronic ID cards. These cards will store electronic signature, biometric data and other administrative data. Currently, there are projects ongoing dealing with the deployment of the eDNI in public administration. Start of the eDNI is expected by the end of this year.
Sweden	no
United Kingdom	ID Card and Citizens Information Card Projects are intended to change current situation. Both projects envisage SIN for natural persons

Question II.5

a) Technical construction of the SIN, b) Can it change over time?

Country	Natural Persons	Legal persons	Can change*	Remark
Austria	12 digits (CRR number) (see remark) 1-11 consecutive number + checksum	consecutive numbers as defined by the associated registers	no/no	From the 12 digit CRR number there is derived the 24 digits "sourcePIN" which is stored on citizen card. Administrations use sector specific PINs derived from this sourcePIN
Belgium	11 digits 1-6 date of birth 7-9 consecutive number + sex 10-11 check sum	10 digits 1: always "0" for enterprises 2-4 VAT office which has issued the number 5-8 consecutive number x digits(?)	no/no	different construction for legal sub entities: 8 digits of consecutive number + 2 digits checksum
Bulgaria	x digits(?) 1-6 date of birth	2-5 legal status 6-7 other parameters of the entity x digits(?)	no/?	
Cyprus	12 digits. 1-2 prefix for Cypriots/non Cypriots. 10 random digits.	random number, prefix indicating legal form x digits(?)	no/no	
Czech republic	10 digits 1-6 date of birth (codes also sex) 7-10 control number		no/?	
Denmark	10 digits 1-6 date of birth 7-10 consecutive number, codes century of birth and sex	-8 digits -1-7 random digits -8 checksum random number	no/no	
France	15 Digits 1 sex 2-5 month and year of birth 6-10 place of birth 11-13 consecutive number 14-15 check key			
Germany Hungary	n/a n/a	SIN for companies: country, legal form, consecutive number SIN for NGOs: year of registration, serial number SIN for budgetary organisations: consecutive number	-/-	The SIN for NGOs changes yearly
Ireland	n/a			

Italy	? Digits codes name, surname, sex, date, place of birth	11 digits 1-7 consecutive number 8-10 competent office 11 control code	yes/no	SIN for natural persons changes when name changes
Lithuania	11 digits 1 sex+century of birth 2-7 date of birth 8-10 consecutive number	9 digits 1-9 random number	no/no	
Luxembourg	11 digits 1-8 date of birth 9-10 digits consecutive number (codes also sex) 11 control number	11 digits 1-4 year of constitution 5-8 legal form 9-11 control digits	no/yes	sin for legal persons changes with legal form
Malta	Maltese citizens: 8 digits 1-5 birth act number 6-7 year of registration 8 letter representing registry and century of registration Non Maltese citizens: 1-7 consecutive number 8 letter A or P	8 digits 2-6 consecutive number 7-8 check number	no/no	New id attributed after naturalisation, old one remains assigned
Netherlands	A-Nr: random number Sofl-Nr: a number that meets the 11-proof	consecutive number 1 code for register of trade	no/no	New "Civil Service Number" will adopt the construction system of the current Sofl-
Poland	11 Digits: 6 birthdate (YYMMDD for person born after 1.1.2000 20 is added to MM) 7-9 place of birth (code) 10 sex	consecutive number the last - check key	no/?	
Spain	8 digits 1-7 random number 8 control number	?	no/?	
Sweden	10 digits 1-6 date of birth 7-9 birth number (codes also sex) 10 check number	10 digits	no/?	
United Kingdom	n/a			

Remark

*Some countries mention the case of error handling and change of the sex. The table does not consider these rare cases.

Question II.6

Which data is linked to the SIN (natural persons)?

Data linked	Austria	Belgium	Cyprus	Czech Republic	Denmark	France	Italy	Lithuania	Luxembourg	Malta	Netherlands	Poland	Spain	Sweden	Bulgaria
name	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
first name(s)	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
sex	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
date of birth	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
place of birth	x	x	x	x	x	x	x		x	x	x	x	x	x	x
address/domicile	x	x	x	x	x				x	x	x	x	x	x	x
former names			x	x	x							x			
pub. key dig. signature	x														
signature													x		
academic/other titles	x														
nationality		x	x	x	x				x	x	x	x			
date/place of death		x	x	x								x			
cause of death			x												
occupational information		x	x		x										
marital status		x	x	x					x		x	x			x
id/name of spouse				x					x			x		x	
household members		x													
photograph			x										x		
community			x												
parent's names/ids			x	x	x				x				x		
children				x	x									x	x
religion			x		x										
education			x												
electoral booklet number			x												
social insurance number			x								x				
driver license number			x												
refugee booklet number			x												
military number			x									x			
legal basis for stay			x								x				
remarks			x												
number of birth document												x			x
number of identity card												x			x
imprisonment info					x										
placed under guardianship				x	x										
deprived of legal capacity				x	x										
restriction of stay				x											
other					x						x				

Austria Information stored in "Identity Link" on citizen cards

Belgium Existence of digital certificate is registered

Bulgaria list not complete

Cyprus stores historical information for many fields
not all fields compulsory

Czech republic stores parents ids, detailed history marital status and domicile

Denmark stores historical and detailed information on names, nationality, domicile, marital status

France Name information is not directly stored in SIN database. Date of birth: month and year only

Netherlands Table shows data for "A-Nr". "Sofi-Nr" has similar data (date of birth misses). There is a foreign key to either number in both databases.

Poland Photographs (also signatures) are stored in the part of the system responsible for ID cards & passports. System is ready for storing data on parent's ID but there is no decision on it

Spain First name of parents only

Question III.7
Question III.8

To which persons is the SIN allocated? (natural persons)
What public authority is in charge of the management of the central SIN database? (natural persons)

Country	Persons, time of allocation	When allocated by whom	Database run by
Austria	-Every Austrian resident -Supplementary register for foreigners	-date of birth registration/move to Austria -after request (foreigners, non-resident Austrians) -municipal registration authorities register	CRR' is operated by Federal Ministry of Interior Data collected and maintained by Municipalities
Belgium	-All residents (registered in three different registers : Belgium, foreigners, refugees) -Special registers for non-residents	-date of birth registration by municipalities -non-residents: first contact with authorities	"Registre National", falls under Ministry of Interior
Bulgaria	-all persons -additional numbers for foreigners(migrants, refugees etc.)	-date of birth registration	General Directorate "Civil Registration" under the Ministry of Regional Development
Cyprus	-persons born in Cyprus -foreign workers in the Cyprus labour market pension fund -persons who have their tax affairs handled in Cyprus	-date of birth registration for residents by Ministry of Interior	Cyprus Civil Registration System, managed by Civil Registry Department, falls under Ministry of Interior
Czech republic	-every Czech or foreign resident	-date of birth registration by municipalities (registry offices)	Ministry of Interior
Denmark	-all persons born in Denmark -foreign workers in the Danish labour market Pension Fund -persons who have their tax affairs handled in Denmark	-date of moving in (foreigners) -date of birth registration by municipalities	"Danish Civil Registration System" is managed by Ministry of the Interior and Health in cooperation with the municipalities
France	all persons born in France/French Overseas Territory	-date of birth by INSEE	Direction INSEE under the Ministry of Economy and Finance
Italy	-every resident	-date of birth registration by municipalities	Ministry of Finance
Lithuania	-every citizen -every resident -persons registering change of civil status in Lithuania	allocated by the "Population Register", approved by Ministry of Interior	Population Register under the Ministry of Interior
Luxembourg	-social security members -"persons registered by any other administration" -every citizen -migrant workers/foreigners if they register	-date of birth or immigration -date of registration -registered by "National Centre for Informatics" -date of birth registration -date of registration	Run by "State Centre for Informatics"
Malta	-A-Nr: -every resident (minimum 4 months stay in 6months time) -persons born in the NL if parent has an A-Nr. Sofit-Nr.: -All persons liable for tax -All persons insured/entitled to benefits in the social sec. System.	-date of registration	Run by "Department of Civil Registration", depends also on "Electoral Office" and "Public Registry".
Netherlands	-every citizen -every resident (after 2 months of stay) -persons registering change of civil status in Poland -every citizen -foreign residents have special ID (NIE)	-date of registration -registered by municipalities Sofit-Nr.: -birth, moving, commencement of liability for tax -registered automatically in the Tax Board Database allocated by the "Population Register", approved by Ministry of Interior - called PESEL	A-Nr.: No centralised database - local government register and maintain decentralised databases. Maintenance of network done by central "Personal Documents Agency" under Ministry of Interior and Kingdom Relations. Sofit-Nr.: Centralised database run by Tax-Office
Poland	-every citizen -every resident (after 2 months of stay) -persons registering change of civil status in Poland -every citizen -foreign residents have special ID (NIE)	allocated by the "Population Register", approved by Ministry of Interior - called PESEL	Population Register under the Ministry of Interior
Spain	-every citizen -foreign residents have special ID (NIE)	-date of issue of the national identity card -compulsory for anyone older than 14 -possible as of birth	Run by Ministry of Interior
Sweden	-every resident (minimum one year stay for foreigners) -children born in Sweden if parent is registered	-date of birth in maternity clinic, final number registered by Swedish National Tax Board -Foreigners when registered	Swedish Population register administered by Swedish National Tax Board. Swedish Person Address Register holds excerpt from national register.

Question III.9a

Which other central registers may access, store and process the SIN /technical realisation?

Country	Person	Registers	Technical realisation
Austria	natural	-hybrid system provides sector specific IDs derived from one central id. Only these can be stored by administrations	-One central SIN, mathematical derivation of sector specific ids
	legal	No restrictions for SINs of legal persons apply	
Belgium	natural	Central administrative network for data exchange using SIN (both for natural and legal persons) as identifier is being built up All administrations will associate to this system	Message oriented electronic system.
	legal		
Bulgaria	natural	-three level hierarchical system (central/federal/municipality) with	
	legal		
Cyprus	natural	-SIN is primary key in almost all government IT systems, secondary	-no technical exchange of data, but ID is locally used
	legal		
Czech republic	natural	-SIN is used in several registers (driving license, statistical service, insurance, banks, hospitals, city transport companies etc.)	
	legal		
Denmark	natural	-Law authorises official authorities to process SIN data -Special regulations for private bodies and individuals apply	
	legal	-SIN for legal persons use required by law for all registers of public authorities	Online access or through other channels
France	natural	-Social security -"Wage" systems -"public" identifier (legal persons)	
	legal		
Germany	n/a		
	natural	n/a	
Hungary	legal	legal persons: one central company register that is public budgetary register: on the internet soon NGO register: available by the County Courts	see left
	n/a		n/a

			all public registers have to adopt the SIN - hence store and process them	different ways
Italy	natural			
	legal			
Lithuania	natural		-widely used by public registers (law regulations apply) -Listed Registers are: Real Property, Tax Payers', Mortgage, Physicians, State Enterprise Centre of Register, State Civil Servants', Guns', State Register of Personal Data Controllers, Vehicles owners, Patient Fund, Customs, etc.	Data accessed via secure communication path on a regular basis using Oracle Snapshot technologies
	legal		-Real property register, Social Insurance, Taxpayers', Register of Education Institutions, Customs	on-line access, replication snapshot, replication XML format
Luxembourg	natural		-all public registers/authorities if required by Law	all modifications are propagated/communicated by National identity register
	legal		-all public registers/authorities if required by Law	all modifications are propagated/communicated by National identity register
Malta	natural		-Public registers may access central SIN database (CdB)	
	legal		-Private entities may purchase data in restricted form -Public registers may access central SIN database (CdB)	
Netherlands	natural		A-Nr: Institutions subscribed to the GBA (Municipal Personal Record DB, accessed data is restricted according to authorisation) Sof-Nr.: Some exchange mainly for control reasons	
	legal			
Poland	natural		-SIN is used in several registers (driving license, taxpayers, vehicle owners, statistical service, business registers, insurance, banks, hospitals, education system, city transport companies etc.)	off-line except the Police, Border Guard - planned to be changes as soon as possible
	legal		-Real property register, Social Insurance, Taxpayers, Customs	off line
Spain	natural		-direct access to central SIN db not allowed	
	legal		-local storage of SIN is foreseen for every public authority	
Sweden	natural		-Person Address Register holds an excerpt from central DB -public authorities are allowed to process the SIN	-made available electronically to public and private bodies
	legal		-Swedish Trade and Industry Register delivers information	-online access
United Kingdom	n/a		n/a	

Question III.9b

Which specific documents comprise the SIN?

Country	Documents
Austria	-Certificate of residence comprises CRR -sourcePIN (see text) stored only on Citizen Card (not human readable) -sector specific PIN can be stored in corresponding sector databases
Belgium	-National identity card (upon request by holder) -Passport (upon request by holder) -Social security card /health card (compulsory) -driving license (being prepared) -tax declaration, school and university inscription, all social security forms
Bulgaria	-All personal documents, e.g. Passports, ID Cards, Driver Licenses, Diploma
Cyprus	-National identity card -health cards -driving license -tax statements and notifications -documents for enrolling children at school and university -many other documents (wide use in society)
Czech republic	-Identity cards, passports -health insurance card -city transport cards (long-term tickets)
Denmark	-Identity cards, passports -social security card / health card -driving licenses -tax statements and notifications documents for enrolling children at school or at university -many other documents (widely used in society)
France	-Social security card -salary statement
Germany	n/a
Hungary	n/a
Ireland	n/a
Italy	-Electronic identity card -National Service Card -Health Insurance Card
Lithuania	-passport, identity card -social security certificate, -driver licence -state civil servant certificate, patient card, pensioner card for personal identification number
Luxembourg	-Social security card
Malta	documents referring to persons include ID number
Netherlands	-Passport, identity card, driving licence: Sofi-Nr. (A-Nr. is used back-office only - not shown on any document)
Poland	-National identity card -Passport -driving license (being prepared)
Spain	appears on rather any document (public/private) with personal data
Sweden	passports, ID-cards, patients' cards
United Kingdom	n/a

Question IV.10

Which national laws, regulations and administrative provisions were brought into force to comply with art. 8.7 of the Directive 95/46/EC?

Country	Documents
Austria	<ul style="list-style-type: none"> - Austrian E-Government Act, Federal Law Gazette part I no. 10/2004 (E-Gov-Act) introduces the sourcePIN system and its mathematical derivations -Section 3 of E-Gov Act regulates that unique identification (by sourcePIN) is only legally allowed insofar as it is necessary in an overriding legitimate interest of the controller, in particular, where it is an essential requirement for performing a task prescribed by law. - General Social Insurance Act, Federal Law Gazette no. 189/1955 (GSI-Act) introduced a Social Security Number (SSN). SSN was brought into life to facilitate the administration of personal relevant data within the legally delegated tasks of the system of social security (sect. 31, para 4 no 1 GSI-Act). - Over the years, legislation started to employ SSN contrary to its original purpose, as a nationwide personal identifier
Belgium	<p>Loi du 8 août 1983 organisant un registre national des personnes physiques (Law 8/8/83)</p> <ul style="list-style-type: none"> - art. 2 : An identification number is allocated to each person at her/his first registration in the National Registry. - art. 8 : The authorisation to use the identification number of the National Registry is given by the sectorial committee of the National Registry to the authorities, organisms and persons listed in art. 5 - art 8: In certain cases, an authorization is not required.
Bulgaria	<ul style="list-style-type: none"> - Law on Protection of Personal Data, published 04/01/2002
Cyprus	<ul style="list-style-type: none"> - Processing of Personal Data (Protection of Individuals) Law of 2001 (138/2001), entered in force in November 2001 - No specific provisions on the processing of a national identification number - Most of the public authorities and private organisations, within the exercise of their responsibilities, use/process the number of the identity card
Czech republic	<ul style="list-style-type: none"> Act no. 101/2000 Col. on personal data protection - Spread usage of identification number for natural persons

Denmark	<p>Danish Act on Processing of Personal Data (Act no. 429 of 31 May 2000)</p> <ul style="list-style-type: none"> - Official authorities may process data concerning civil registration numbers with a view to unambiguous identification or as file numbers. - Private individuals and bodies may process data concerning civil registration numbers where (1) this follows from law or regulations; (2) or the data subject has given his explicit consent; (3) or the processing is carried out for scientific or statistical purposes or if it is a matter of disclosing a civil registration number where such disclosure is a natural element of the ordinary operation of companies, etc. of the type mentioned and the disclosure is of decisive importance for an unambiguous identification of the data subject or the disclosure was demanded by an official authority. - Irrespective of the provision laid down in subsection (2) (3), no disclosure may take place of a civil registration number without explicit consent. <p>The civil registration is specifically regulated in Act no. 426 of 31 May 2000.</p>
France	<p>Loi du 6 août 2004 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel et modifiant la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés</p>
Germany	<p>Federal Data Protection Act (Bundesdatenschutzgesetz, BDSG, in the version published on 14 January 2003, Federal Law Gazette I 66)</p> <ul style="list-style-type: none"> - general provisions on how to treat personal data - no specific provisions for general personal identification number because such a number does not exist for natural persons <p>Many rules in place on data protection for specific areas (e.g. social security, tax administration)</p>
Hungary	<p>Special law for the privacy harmonised completely with the Directive 95/46/EC</p> <ul style="list-style-type: none"> - Natural persons cannot be identified by means of a single identification number.
Ireland	<p>Data Protection (Amendment) Act 2003</p> <ul style="list-style-type: none"> - Single identifier (PPSN) was introduced in the 1998 Social Welfare Act as a unique identifier between individuals and the public service. Social Welfare Acts of 1999, 2000, 2002 and 2003 also have provisions governing the use of the PPSN. - In order to use the PPSN an organisation has to have been specified in one of these pieces of legislation. Other organisations can only use the PPSN if they are acting on behalf of one of the specified bodies, are specifically authorised by other legislation or are doing so in order to complete a transaction with a public body. - Using the PPSN to share data between organisations has to be specifically provided for in legislation otherwise it is an offence. - The Police force and the Defence forces can only use the PPSN in respect of their own staff.
Italy	<p>- No answer</p>

Lithuania	<p>Law on Legal Protection of Personal Data (Law LPPD), the Law on Population Register, Regulations of Population Register.</p> <ul style="list-style-type: none"> - the use of a personal identification number for the processing of personal data shall be conditional on the consent of the data subject (Art. 7 of Law LPPD) - the personal identification number may be used when processing personal data without the consent of the data subject only if: <ul style="list-style-type: none"> 1) such a right is stipulated in this Law and other laws; 2) for research or statistical purposes in cases specified in Articles 12 and 13 of this Law; 3) in state registers and information systems provided that they have been officially approved under law; 4) it is used by legal persons involved in activities related to granting of loans, recovery of debts, insurance or leasing, health care and social insurance as well as in the activities of other institutions of social care, educational establishments, research and studies institutions, and when processing classified data in cases provided by law. - There are also other specific Laws which regulates the use of personal identification number in particular sectors.
Luxembourg	<p>Loi du 30 mars 1979 organisant l'identification numérique des personnes physiques et morales</p>
Malta	<p>Data Protection Act 2001 (DPA) enacted on 14/12/2001</p> <ul style="list-style-type: none"> - The identity card number may, in the absence of consent, only be processed when such processing is clearly justified having regard to the purpose of the processing; the importance of a secure identification; some other valid reason as may be prescribed.
Netherlands	<p>Personal Data Protection Act</p> <ul style="list-style-type: none"> - For the processing of personal data a national identification number can only be used for the implementation of the law which states that such a number may be used or for the purpose specified by law.
Spain	<ul style="list-style-type: none"> - Current DNI was first regulated in 1967 - Electronic DNI regulated in the Law 59/2003 on electronic signature - General provisions regarding protection of personal data applies for processing the single identification number
Sweden	<p>Personal Data Act (PDA) (SFS 1998:204), entered into force 24/10/1998</p> <ul style="list-style-type: none"> - repeals Data Act of 1973 - aims at preventing the violation of personal integrity by the processing of personal data
United Kingdom	<p>Data Protection Act 1998 and associated secondary legislation</p> <ul style="list-style-type: none"> - The regime will apply to (for instance) the personal data required for the Identity Card Scheme.

Question IV.11

Which authority is responsible for monitoring the application of the legislation of data protection (Art. 28, directive 95/46/EC)?

Country	Documents
Austria	- Austrian Data Protection Commission (DPC) - System of legal protection in data protection affairs is predominantly reacting - not monitoring - Exceptions: registration duty, obligation to obtain a permission for transborder transmission or special purposes of data use - Monitoring duty conferred upon each individual controller by law. Irrespective of belonging to the private or public sector, controllers face security measures they have to obey Future evolution expected - sourcePIN register Authority (i.e. DPC) likely to log transformation requests for sector specific PINs
Belgium	Commission de la Protection de la Vie Privée (CPVP) + Comités sectoriels
Bulgaria	Commission for Personal Data Protection, whose members are appointed by the Parliament
Cyprus	Commissioner for Personal Data Protection
Czech republic	Office for Personal Data Protection (OPDP) and Ministry of Interior which is responsible for the nation register
Denmark	Danish Data Protection Agency (DPA)
France	Commission nationale de l'informatique et des libertés (CNIL)
Germany	Different authorities: - Data processed by public authorities at Federal level: Federal Commissioner for Data Protection - Data processing by public authorities at Laender level: Land Commissioners for Data Protection - Monitoring data processing by private bodies: Land Commissioners for Data Protection or other authorities assigned by the Laender.
Hungary	The office of the Data Protection and Freedom of Information Commissioner of the Hungarian Parliament
Ireland	Data Protection Commissioner
Italy	no answer
Lithuania	State Data Protection Inspectorate (SDPI)
Luxembourg	Commission Nationale pour la Protection des Données (CNDP)
Malta	Commissioner for Data Protection who is appointed by the Prime Minister after consultation with the Leader of the Opposition
Netherlands	Het College Bescherming Persoonsgegevens (Dutch Data Protection Authority)
Spain	Agencia Española de Protección de Datos (AEPD)
Sweden	Data Inspection Board (DIB)
United Kingdom	The Information Commissioner

Question IV.12a Usage of SIN and exchange of data between administrations making use of SIN, general notification requirement?

Country	Documents
Austria	As a matter of principle, each data application has to be notified to the Austrian Data Processing Register
Belgium	Data processing must be notified in advance to the CPVP
Bulgaria	Yes
Cyprus	- Controllers have an obligation to submit separate notification forms for each separate data processing operation they are carrying out - The exchange of data between Departments of the Central Government or other authorities or organizations is regulated by the provision in the Law about combination of filing systems
Czech republic	-Yes - Required notification in writing prior to commencing personal data processing.
Denmark	No, not on the sole basis that the processing concerns civil registration numbers.
France	Requirement to ask for authorisation to CNIL
Germany	- Obligation to notify supervisory authorities: Sections 4d and 4e of BDSG both for private and public bodies - Any automated processing procedure must be registered with the relevant supervisory authority before it is taken into operation - Specific provisions for public bodies at Länder level
Hungary	Yes
Ireland	- The notification requirement is not related to the processing of the single identifier. - All public sector organisations are subject to the notification requirement which in turn means that virtually all users of the PPSN are required to notify.
Italy	No answer
Lithuania	- Yes. Art. 25 of Law LPPD provides that personal data may be processed by automated means subject to notification by the data controller or his representative of the SPDI
Luxembourg	Yes
Malta	Yes
Netherlands	Not in general.
Spain	The legal instrument (for Public Administrations) or inscription (for private companies) in the AEPD Register, needed to create each personal data file, must specify all personal data (including the identification number if that is the case). But there is not any specific provision in the privacy protection regulation for the management of PIN.
Sweden	- Primary obligation to notify all data processing to the supervisory authority, which must maintain a register of the notifications - Many exemptions from the general notification obligation, e.g. where the processing is regulated in a specific Act or Ordinance, which is the case regarding many databases in public administration
United Kingdom	Yes

Question IV.12b Exceptions to the general notification requirement, cf art. 18.2, Directive 95/46/EC

Country	Documents
Austria	-Exemptions: when the intended data application is listed among the standard applications published by decree of the Federal Chancellor (Standard and Model Applications Decree 2004)
Belgium	Exemptions: - by legislative act, when, according to the processed data, there is evidently no risk to affect the rights and freedoms of the concerned persons, and if are mentioned the purpose of the data processing, the categories of data processed, the categories of concerned persons, the categories of data recipients and the duration of conservation of the data
Bulgaria	No answer
Cyprus	Exemptions: - provided by section 7(6) of the Law - does not include the exemption stated in the questionnaire
Czech republic	Exemptions: - personal data that are part of data files publicly accessible on the basis of a special Act - personal data imposed on the controller by a special Act or when such personal data are needed for exercising rights and obligations following from a special Act - in case of processing that pursues political, philosophical, religious or trade- union aims carried out within the scope of legitimate activity of an association and which relates only to members of the association or persons with whom the association is in recurrent contact related to legitimate activity of the association, and the personal data are not disclosed without the consent of data subject
Denmark	No
France	Exemptions: - for processing related to public security
Germany	-Exemptions: - If the responsible body has appointed its own data protection official, obligatory registration is replaced by the obligation to notify this data protection official of the relevant procedure
Hungary	Yes
Ireland	- no exemptions for in-house data protection officials - no other exemptions that public sector organisations can avail of
Italy	No answer
Lithuania	Exemptions: - processing for the purposes of internal administration - processing is carried out in the course of the activities by a foundation, association or any other non-profit-seeking body for political, philosophical or trade union aim on condition that the processed data relate solely to the members of the body or to persons who have regular contact with it in connection with its purposes - processing of personal data with provision of information to the public - processing of personal data for purposes of health care - following the procedure set forth in the Law of the Republic of Lithuania on State and Official Secrets
Luxembourg	Yes
Malta	Yes, where a Personal Data Representative is appointed. However, the Personal Data Representative has to forward all registration details and notification fees collected to the Commissioner.
Netherlands	If there is a personal data protection official the notification can take place with him.
Spain	No answer
Sweden	- Government or DIB may issue regulations concerning exemptions for such kinds of processing as are not likely to result in an improper violation of personal integrity. - Other exemptions are found in the Personal Data Ordinance and the Data Inspection Board Code of Statutes
United Kingdom	- There are exemptions but usage of the single identification number would not fall into that category. - The appointment of a Personal Data Protection Officer is uncommon.

Question IV.12c

Personal data processing subject to prior checks, cf art. 20, Directive 95/46/EC

Country	Documents
Austria	- Prior check necessity is assessed for the whole data application. No specific evaluation for personal identifiers
Belgium	- The categories of data processing that present specific risks concerning the rights and freedoms of the concerned persons are submitted to particular conditions
Bulgaria	No answer
Cyprus	No
Czech republic	- If a justified concern arises, OPDP shall initiate proceedings at its own instigation.
Denmark	No
France	Prior notification to CNIL, which may assess if the processing is legitimate
Germany	No answer
Hungary	Yes
Ireland	No
Italy	No answer
Lithuania	SDPI shall carry out prior checking in the following cases: - where the data controller intends to process special categories of personal data save (purposes of health care, for the prevention and investigation of criminal offences, and data necessary for a court hearing) - where the data controller intends to process public data files unless the laws and other legal acts specify the procedure for disclosure of the data - where the data controller of the information systems of state registers or state and municipal institutions authorises the data processor to process personal data save the cases where the laws and other legal acts provide for the right of the data controller to authorise a specific data processor to process personal data or where the data processor is a legal entity established by the data controller - processing of personal data for purposes of scientific research without the consent of data subject, processing of personal data for the purposes of evaluation of a person's solvency and management of his debt, and processing of personal data for the statistical or research
Luxembourg	Yes
Malta	- All processing operations that involve risks of improper interference with the rights and freedoms of data subjects are to be submitted for prior checking by the Commissioner.
Netherlands	Prior checking is obliged when the id-number is used for other purposes than described by law.
Spain	No answer
Sweden	- Government may issue regulations that particularly sensitive processing must be notified to the supervisory authority for prior examination three weeks in advance. This applies even if a data representative has been appointed.
United Kingdom	No

Question IV.13a

National realisation of information and notification right, access right and right to object

Country	Documents
Austria	<p>Information and notification right</p> <ul style="list-style-type: none"> - cf. sections 24 and 25 of the Austrian Data Protection Act (DPA) - Controller has to inform the data subjects when collecting data in an appropriate manner about the purpose of the data application for which the data is collected, and the name and address of the controller - In case of data application subject of notification, communication to the data subject shall carry the controller registration number <p>Access right</p> <ul style="list-style-type: none"> - cf. section 26 of DPA - Controller shall provide the data subject with information about the data being processed and relating to him, if the data subject so requests in writing and proves his identity - The information shall contain the processed data, the available purpose of the use of data, its legal basis in an intelligible form - Upon request of the data subject, the names and addresses of processors shall be disclosed in case they are charged with processing data relating to him <p>Right to object</p> <ul style="list-style-type: none"> - cf. Section 28 of DPA - Insofar as a use of data is not authorised by law, data subject is entitled to raise a founded objection against this use of data because of an infringement of overriding interests in secrecy. - If requirements are met, controller obliged to erase the affected data within eight weeks
Belgium	<p>Implemented in the Law of 8/12/1992 concerning the protection of personal data</p> <p>Information and notification right</p> <ul style="list-style-type: none"> - cf. Art 9 para. 1 - The controller or his representative must provide the concerned person, at the latest when the data are obtained, at least the following information: the name and address of the controller (or his representative); the purpose of the processing; the information about his right to oppose to the processing for direct marketing; some complementary information such as the recipient of the data, the mandatory or optional nature of the answers, the information about the right to access and the right to correct the data; other information linked to the specific nature of the processing <p>Access Right</p> <ul style="list-style-type: none"> - cf. art. 10. para. 1 - After having proved its identity, a person has the right to obtain from the controller: the confirmation that some data concerning him/her are or are not processed, as well as information about the purpose of the processing, the categories of data processed, the
Bulgaria	<p>No answer</p>
Cyprus	<p>Information and notification right</p> <ul style="list-style-type: none"> - Data subjects, at the time of collection of their personal data by the controller, have to be informed about the controller's identity and the purpose of the processing. They should also be informed about the recipients or the categories of recipients of the data, the existence of the right of access and rectification, whether they are obliged to provide assistance and the consequences of their refusal, if this information is necessary in order to guarantee legitimate processing. - Some derogations to this right: processing performed for statistical, historical and purposes of scientific research, for purposes of defence, national security of the Republic or for the prevention, detection or investigation and prosecution of criminal offences provided that a license is issued by the Commissioner <p>Access Right</p> <ul style="list-style-type: none"> - Data subjects have the right to ask: 1. information on their personal data processed by the controller i.e. source, recipients, purpose and progress of processing, 2. rectification, erasure or

Czech republic	<p>Act 101/2000</p> <p>Information and notification right</p> <ul style="list-style-type: none"> - The data subject has an information and notification right - Exceptions: <ul style="list-style-type: none"> personal data processing for statistics, scientific research, archives... personal data processing imposed by a special Act processing lawfully published personal data processing personal data obtained with the consent of data subject <p>Access right</p> <ul style="list-style-type: none"> - The data subject has a access right <p>Right to object</p> <ul style="list-style-type: none"> - The data subject has the right to have his personal data rectified
Denmark	<p>Danish Act on Processing of Personal Data</p> <p>Information and notification right</p> <ul style="list-style-type: none"> - Section 28-30 <p>Access right</p> <ul style="list-style-type: none"> - Section 31 <p>Right to object</p> <ul style="list-style-type: none"> - Section 35 and 36
France	<p>Loi informatique et libertés</p>
Germany	<p>Bundesdatenschutzgesetz (BDSG)</p> <p>Information and notification right</p> <ul style="list-style-type: none"> - The data subject must be informed of the circumstances of data processing, if personal data of this person is collected. - If data is collected without the data subject's knowledge, he/she must be informed. <p>Access right</p> <ul style="list-style-type: none"> - The person concerned has a right of access. <p>Right to object</p> <ul style="list-style-type: none"> - The person concerned has the right to object. <p>At Laender level</p> <ul style="list-style-type: none"> - Data processing by public authorities of the Laender are governed by provisions of the respective data protection legislation of the Laender - Those rights are implemented by special laws (e.g. regulations on electronic health card)
Hungary	<p>Information and notification right</p> <ul style="list-style-type: none"> - The data subject shall be given unambiguous and detailed information on all the facts relating to the processing of his data, in particular on the purposes and legal basis of the data processing, on the person authorised to carry out the data processing and the technical data processing, the duration of data processing, as well as on who is authorised to have access to the data. Information shall also be given on the rights and remedies of data subjects in connection with the data processing. - The information on data processing shall be considered to have been given where a rule of law orders the collection of data from an existing data file by transfer or combination. - If impossible / too expensive to inform each data subject (e.g. statistics or scientific purposes), information may be given by making public, in a way that it will be accessible to all, the fact of data collection, the data subjects concerned, the purpose of the data collection, the duration of the data processing, and the accessibility of the data.
Ireland	<p>Data Protection Acts (DPA)</p> <p>Information and notification right</p> <ul style="list-style-type: none"> - Data subject has this right <p>Access right</p> <ul style="list-style-type: none"> - right of access to personal data held electronically or in a relevant filing system. - Some exemptions but these would not especially hinder an individual's right to access information held under the single identification number. <p>Right to object</p> <ul style="list-style-type: none"> - right to object to processing where it is carried out on the basis that it is in the public interest or in the exercise of public authority or on grounds that it is in the legitimate interests of the data controller. - grounds for objection: the processing would cause substantial unwarranted damage or distress. - right to object does not apply where the data controller is acting under a legal obligation.
Italy	<ul style="list-style-type: none"> - No answer

Lithuania	<p>Law on Legal Protection of Personal Data (art. 17, 18, 19, 21)</p> <p>Information and notification right - Data subject has the right to know/ be informed about the processing of his personal data</p> <p>Access right - Data subject has the right to have access to his personal data and familiarise himself with the processing method</p> <p>Right to object - Data subject has the right to demand rectification or destruction of his personal data or restriction of further processing of his personal data, with the exception of storage, where the data are processed not in compliance with the provisions of this Law and other laws - Data subject has the right to object to the processing of his personal data</p>
Luxembourg	<p>Information and notification right - The persons registered in the General Register are informed of the registration, modification or corrections of data concerning them.</p> <p>Access right -</p> <p>Right to object - Any person registered in the General Register may request a modification or a correction of his/her data, providing that he/she provides the required justification</p>
Malta	<p>Information and notification right -Data subjects are to be provided with details concerning the identity and address of the controller, together with the purpose for processing, recipients, obligatory or voluntary replies to questions, and existence of right of access.</p> <p>Access Right - The data subject has also the right to obtain written information concerning him/her, without excessive delay and without expense.</p> <p>Right to object - The data subject has the right to rectify, block or erase such personal data that has not been processed in accordance with the Act</p>
Netherlands	<p>- Those rights are described in the data protection law. Data subjects use their rights incidentally.</p>
Spain	<p>- Rights realised according to the Ley Orgánica 15/1999 de Protección de Datos de Carácter Personal and related regulation</p>
Sweden	<p>Information and notification right - The controller is liable to provide, free of charge, notification once per calendar year concerning whether personal data relating to a particular person has been processed or not, provided the person so requests.</p> <p>Access right - If such data is processed, written information shall be provided about which data concerning the applicant is processed, where the data has been collected, the purpose of the processing and to which recipient or categories of recipients the data is disclosed.</p> <p>Right to object - cf sections 11, 12 of PDA</p>
United Kingdom	<p>Information and notification right - ?</p> <p>Access right - Right of access to data</p> <p>Right to object - Right of rectification, removal or erasure if ordered by court - Right to prevent processing likely to cause damage or distress</p>

Question IV.13b

Right to access: online access?

Country	Documents
Austria	<ul style="list-style-type: none"> - Concrete design of the process to access data is not regulated by law - Written proof of identity is mandatory - Online processing not impeded by legal requirement because Law on General Administration Procedure 1991 puts written documents on a par with online doc.
Belgium	<ul style="list-style-type: none"> Law of 19/07/1991 relative to the registry of population and to the identity cards - The person which is titular of the electronic identity card may ask which data are stored on the card and which data may be accessed with the card. - The person which is titular of the electronic identity card may also ask this information to the township where he is registered on the Register of population. - Online access is allowed. Authentication is achieved via the identification certificate stored on the electronic identity card.
Bulgaria	<ul style="list-style-type: none"> - Operation realised as e-Service 'on-line' but the access to the service is admitted only with e-certificate
Cyprus	<ul style="list-style-type: none"> - The Access right is exercised by submitting an application directly to the controller. - Currently no online access is provided to neither individuals nor Government Organizations. - Government organizations after the necessary approval by the Commissioner are provided with the required information on other electronic means (CDs) .
Czech republic	<ul style="list-style-type: none"> - No answer
Denmark	<ul style="list-style-type: none"> - Online access to the personal data is possible for some registers but requires a personal electronic signature or a pin code - No right to have online access but right to receive the information in writing
France	<ul style="list-style-type: none"> - Person may access his data, but not online in all cases
Germany	<ul style="list-style-type: none"> - The responsible authority exercises due discretion in determining the procedure for providing information - Private bodies must provide such information in writing unless special circumstances warrant any other form - Under development: architecture and concepts for access to electronic healthcare records and other data managed by the use of an electronic health card
Hungary	<ul style="list-style-type: none"> - The registers of legal persons are public. - The company register can be accessed online. - The register of the budgetary institution will be accessible online soon. - Natural persons cannot be identified by means of a single identification number.
Ireland	<ul style="list-style-type: none"> - Not Applicable
Italy	<ul style="list-style-type: none"> - No answer
Lithuania	<ul style="list-style-type: none"> - Proof of identity is mandatory - Request to the controller - Information must be provided to the data subject in writing.
Luxembourg	<ul style="list-style-type: none"> - Not yet
Malta	<ul style="list-style-type: none"> - Personal data can be accessed both on-line and in report format, as long as it is intelligible information. Such access depends on the facilities and functionality offered by different applications.
Netherlands	<ul style="list-style-type: none"> - Individuals in general do not have access to his data online.
Spain	<ul style="list-style-type: none"> - General procedure applies, including telematic access when available.
Sweden	<ul style="list-style-type: none"> - An application for information shall be made in writing to the controller and signed by the applicant personally - If the controller is a public authority, the concerned person would normally have a right to access her own information under the freedom of information regulation. - The concerned person has no general right to access data concerning herself if that data is held by a controller other than a public authority. - Access must not be provided if the information is confidential according to the Secrecy Act. - In some cases determined by Government, the concerned person may have direct access to information about itself
United Kingdom	<ul style="list-style-type: none"> - Since January 2005, possible to request access to data held by written request (including email). The information may be sent electronically to the person making the request. There may well be cases where the information is only held electronically.

Question IV.14a

Transfer, sharing, interconnection and exchange of personal data between admin. Requirement for explicit authorisation?

Country	Documents
Austria	- No, regardless of the constitutional principle that every usage of data by a public authority requires the legal form of an act, no additional authorisation needed due to the use of new identifiers - Existing rules of data protection are sufficient
Belgium	- An authorisation from the relevant 'comité sectoriel' is needed for each data flow - There is need for different authorisations if the public interest and the purpose are different. Mostly the fact that it is about a different administration will justify a different authorisation
Bulgaria	- No answer
Cyprus	-No. The provisions of the general Data Protection Law cover all cases stated in this question.
Czech republic	?
Denmark	- Public authorities must have authorisation in Danish law, foremost the Act on Processing of Personal Data
France	- Yes, a specific and explicit authorisation is required.
Germany	-Public authorities are solely allowed to process and transmit data, if the person concerned has consented to this or a law permits or prescribes data processing - A legal power to transfer personal data can be inferred for public authorities in certain circumstances Specific identification numbers: - The identification number of natural persons used for tax purposes must not be used by other authorities - The business identification number used for tax purposes will be designed for future use also by other authorities
Hungary	-Natural persons do not have single identification numbers. Authorities can transfer, share, interconnect personal data by means of connection code if they are authorised to do it by a specific law. - The data of legal persons can be transferred, shared, interconnected by using the single identification number without any restriction unless they are confidential.
Ireland	- The sharing of data using the single identifier has to be provided for in law. (restriction imposed by the Social Welfare Acts 1998 – 2003).
Italy	- No answer
Lithuania	- Yes, cf. question 10
Luxembourg	- Yes
Malta	- No, as long as this is in line with article 18 of the DPA and appropriate notification of the processing operations has been made in line with the notification procedures
Netherlands	- Yes, exchange of personal data between public agencies has to be authorised by a specific law.
Spain	- Yes. In the case of Public Administration, it should be specified any sharing or exchange of personal data in the legal provision that creates the electronic administrative procedure. It should be also included in the legal instrument that creates or modify the file
Sweden	- In most cases, exchange of data between agencies is governed by sector specific data protection laws ("database acts") and regulations. - Processing of personal data within public agencies or administrative authorities is often specifically regulated - If there is no specific Act or Ordinance that regulates this, the general provisions in the PDA apply - Exchange of data between public agencies and administrative authorities is also regulated by the Secrecy Act
United Kingdom	- Unknown whether data-sharing does happen by using a common single identifier to bring together the relevant datasets. - No specific regulatory requirement that would apply to the use of this number. - The actual disclosure or sharing of data would be subject to the Data Protection Regulatory Framework and to other applicable law

Question IV.14b Transfer, sharing, interconnection and exchange of personal data between admin. Authority for data protection asked for comment?

Country	Documents
Austria	- No - referring to eldentities, DPC just logs the transforming applications and stores them for possible ex-post audit - Yes - referring to general concerns of data protection, DPC is involved, insofar it has some
Belgium	- Yes, indirectly via the 'comités sectoriels' of which half of the members are members of the CPVP
Bulgaria	- No answer
Cyprus	- Yes. According to section 8 and 9 of the Law on combination of filing systems and transfer of data to third countries, the Commissioner issues the relevant licenses after the submission of an application. Regarding the combination of filing systems a hearing of the controllers is
Czech republic	?
Denmark	- No
France	- Yes
Germany	- The authority monitoring compliance with data protection provisions does not need to authorise the transmission of data in advance - Exception of obligatory registration if data protection official is appointed (cf. Q12b)
Hungary	- During the legislation the Data Protection and Freedom of Information Commissioner has to be asked.
Ireland	- not compulsory but in practice there is consultation on the general principles
Italy	- No answer
Lithuania	- No
Luxembourg	- No - Yes
Malta	- Only in cases where there is a risk of improper interference with the rights and freedoms of the individual
Netherlands	- No.
Spain	- Private sector: approval of the AEPD is necessary before the creation of the file. - Public sector: prior authorisation it is not formally compulsory, but final word remain at the AEPD, eventually.
Sweden	- Not mandatory - DIB is usually consulted on proposals for legislation - DIB does not issue authorisations.
United Kingdom	- No answer

Question IV.14c Transfer, sharing, interconnection and exchange of personal data between admin.
Specific provisions for cross-border transfers?

Country	Documents
Austria	-No - The same data protection rules that would be applied without using these personal identifiers, would be executed in case of using them
Belgium	- Yes, the non-EU country must assure an adequate level of personal data protection - Some exceptions are possible (e.g. explicit agreement of the concerned person...)
Bulgaria	- No answer
Cyprus	-Yes. The provisions are stated in section 9 of the Law.
Czech republic	?
Denmark	- No transfer of data outside the EU may take place without a specific legal basis in Section 27 of the Act. - In some cases this may require prior authorisation from the DPA. Furthermore, Section 11 of the Act, as cited above, must always be complied with when transferring data regarding the civil registration number both within the EU and outside the EU.
France	- Yes
Germany	-Additional requirements must be met for the transmission of data to authorities outside the scope of Directive 95/46/EC (authorities in Non-EU Member States or EU authorities outside the scope of application of the Directive)
Hungary	- No personal data (including special data) shall be transferred in non-EU countries without the data subject's consent or unless provided for by an Act or an international agreement, and even then only where the legislation of the third country guarantees adequate protection.
Ireland	- No specific provisions. The normal data protection rules governing transfers abroad would apply.
Italy	- No answer
Lithuania	- Transfer of personal data to recipients in foreign countries shall be subject to an authorisation from the SDPI, except in certain cases. - Without an authorisation of the SDPI personal data shall be transferred to a third country or an international law enforcement organisation only if: 1) the data subject has given his consent to the transfer of the data; 2) the transfer of personal data is necessary for the conclusion or performance of a contract between the data controller and a third party concluded in the interests of the data subject; 3) the transfer of personal data is necessary for the performance of a contract between the data controller and the data subject or the implementation of pre-contractual measures taken in response to the data subject's request; 4) the transfer of personal data is necessary or legally required in the public interest or for the purpose of legal proceedings; 5) the transfer is necessary in order to protect the vital interests of the data subject; 6) the transfer is necessary for the prevention or investigation of criminal offences; 7) the data are transferred from a public data file following the procedure prescribed by laws an
Luxembourg	- Yes
Malta	- Non-EU countries are subject to a specific provision which states that the third country must ensure an adequate level of protection, to be determined by the Commissioner.
Netherlands	- See directive
Spain	-According to European Directive provision
Sweden	- No specific provisions as regards transfer within the EU - Transfer outside the EU is in principle regulated in the PDA and in the Personal Data Ordinance. - If the processing is specifically regulated, this regulation may also contain rules on third country transfers.
United Kingdom	- No answer

Question IV.15

Shared databases allowed by law?

Country	Documents
Austria	<ul style="list-style-type: none"> - Yes. - The concrete requirements to meet are defined by the DPC, which performs the prior check of these joint information systems - The controllers of a joint information system have to appoint a suitable operator for the system, unless one is already regulated by law (cf. Sect. 50 of DPA) - Name and address of the operator shall be included in the notification for registration - The operator shall be responsible for the necessary data security measures in the joint information system - Further controller duties may be assigned to the operator by an appropriate legal instrument
Belgium	<ul style="list-style-type: none"> - Yes, shared databases are allowed, providing that they meet the basic principles related to their purpose and the proportionality and that they are authorised by the CPVP - Shared databases must be kept up-to-date and cannot be considered as reference data
Bulgaria	<ul style="list-style-type: none"> - No answer
Cyprus	<ul style="list-style-type: none"> - There is no specific provision in the Law on the construction of shared databases.
Czech republic	<ul style="list-style-type: none"> - No but the registers can exchange data (as it is stated in the legislation)
Denmark	<ul style="list-style-type: none"> - Yes, if there is an authorisation by a specific law and again if it is within the Directive 95/46/EC. - The law should accurately state who has the authorisation to access or exchange the specific personal data and to what purpose.
France	<ul style="list-style-type: none"> - Loi informatique et libertés + CNIL
Germany	<ul style="list-style-type: none"> - In general, shared databases of different public authorities are not allowed - Possibility of shared databases, but requires that ... <ol style="list-style-type: none"> 1) the procedure is in due regard to the legitimate interests of the data subject and to the duties or business purposes of the bodies involved 2) appropriate measures are taken to ensure that the admissibility of individual access can be monitored at all times - Federal Commissioner for Data Protection must be notified in advance
Hungary	<ul style="list-style-type: none"> - Databases containing personal data cannot be shared. - Common entities – if they are personal data – can be transferred for harmonization purposes only if it is authorised by law.
Ireland	<ul style="list-style-type: none"> - No answer
Italy	<ul style="list-style-type: none"> - No answer
Lithuania	<ul style="list-style-type: none"> - Yes, but the Law on LPPD and special legislation are applied. - Basic Data Protection principles: Personal data must be: <ol style="list-style-type: none"> 1) collected for specified and legitimate purposes determined before collecting personal data and are later processed in a way compatible with those purposes; 2) processed accurately, fairly and lawfully; 3) accurate, and, where necessary for the processing of personal data, kept up to date; inaccurate or incomplete data must be rectified, supplemented, destroyed or their further processing must be restricted. 4) identical, adequate and not excessive in relation to the purposes for which they are collected and processed; 5) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the data were collected and processed. - The specific provisions concerning the recipients, the purposes of the processing, the legal ground of the processing, the sources of the data, the users of the data, the suppliers of the data must be clearly stated in the laws or in the secondary legislation.
Luxembourg	<ul style="list-style-type: none"> - The interconnection of data is allowed by the Law of 06/08/2002 - Requires the prior authorisation of CNPD

Malta	<ul style="list-style-type: none"> - Such databases can be deployed where it is in the legitimate interest of the public authorities, and when this is made in a lawful manner. - Personal details which fall under the public domain can be shared. - Also, such access is allowed in cases where it is specifically provided for by law (for the purposes of taxation, detection and prevention of crime, national audits and investigation, national security and defence).
Netherlands	<ul style="list-style-type: none"> - Not in general, but sometimes it is possible.
Spain	<ul style="list-style-type: none"> - General privacy protection applies for personal number identifications
Sweden	<ul style="list-style-type: none"> - No - In specific Acts or Ordinances that regulate specific databases, there are often rules regarding access to information for other authorities.
United Kingdom	<ul style="list-style-type: none"> - Yes (although unsure as to what is meant by the term 'entities') - Unknown whether data-sharing does happen by using a common single identifier to bring together the relevant datasets - The actual disclosure or sharing of data would be subject to the Data Protection Regulatory Framework and to other applicable law

Question IV.16a Can the SIN be used by private bodies for their internal use?

Country	Documents
Austria	<ul style="list-style-type: none"> - The sourcePIN must not be used for natural persons - Private bodies can use a sector specific PIN derived from the source PIN. With private bodies, the sector is the body itself, i.e. the same person has different ssPIN within the databases of different private bodies - Private bodies can ask for an identifier especially designed for the private sector, called private sector specific PIN (pssPIN) - The construction process of ssPIN (public sector) and pssPIN (private sector) are different
Belgium	- No
Bulgaria	- Yes
Cyprus	- The identity card number may be used.
Czech republic	- Yes, if the citizen agree then yes, but should be changed
Denmark	<ul style="list-style-type: none"> - Private individuals and bodies may process data concerning civil registration numbers where <ol style="list-style-type: none"> (1) this follows from law or regulations; (2) or the data subject has given his explicit consent; (3) or the processing is carried out for scientific or statistical purposes or if it is a matter of disclosing a civil registration number where such disclosure is a natural element of the ordinary operation of companies, etc. of the type mentioned and the disclosure is of decisive importance for an unambiguous identification of the data subject or the disclosure was demanded by an official authority. - Irrespective of the provision laid down in subsection (2) (3), no disclosure may take place of a civil registration number without explicit consent.
France	<ul style="list-style-type: none"> - Yes for legal persons - No for natural persons
Germany	- N/A
Hungary	<ul style="list-style-type: none"> - Natural persons have no single identification numbers. - The single identification numbers of legal persons can be used by anybody without any restriction.
Ireland	- No answer
Italy	- No answer
Lithuania	- No
Luxembourg	- No
Malta	-Yes, as long as it is in line with article 18 of the DPA
Netherlands	- For the processing of personal data a national identification number can only be used for the implementation of the law which states that such a number may be used or for the purpose specified by law.
Spain	- Yes
Sweden	- Yes, with consent or based on any of the other grounds in section 9 of the PDA
United Kingdom	- No answer

Question IV.16b Can the SIN be used in contacts between private bodies and citizens?

Country	Documents
Austria	- idem 16a because no legal distinction is made by law between private bodies and citizens.
Belgium	- No
Bulgaria	- Yes
Cyprus	- The identity card number may be used.
Czech republic	- Yes
Denmark	- Private individuals and bodies may process data concerning civil registration numbers where (1) this follows from law or regulations; (2) or the data subject has given his explicit consent; (3) or the processing is carried out for scientific or statistical purposes or if it is a matter of disclosing a civil registration number where such disclosure is a natural element of the ordinary operation of companies, etc. of the type mentioned and the disclosure is of decisive importance for an unambiguous identification of the data subject or the disclosure was demanded by an official authority. - Irrespective of the provision laid down in subsection (2) (3), no disclosure may take place of a civil registration number without explicit consent.
France	- Yes for legal persons - No for natural persons
Germany	- N/A
Hungary	- Natural persons have no single identification numbers. - The single identification numbers of legal persons can be used by anybody without any restriction.
Ireland	- No answer
Italy	- No answer
Lithuania	- Yes
Luxembourg	- No
Malta	- Yes, as long as it is in line with article 18 of the DPA
Netherlands	- For the processing of personal data a national identification number can only be used for the implementation of the law which states that such a number may be used or for the purpose specified by law.
Spain	- Yes
Sweden	- Yes, with consent or based on any of the other grounds in section 9 of the PDA
United Kingdom	- No answer

Question IV.16c Can the SIN be used in contacts between private bodies and public administration?

Country	Documents
Austria	- Possible, yes but the public administration has to ask the source PIN registration authority to calculate its ssPIN from the ssPIN provided by the private body - Transmission of ssPIN is prohibited by law, unless the ssPIN is required for identification purposes and shall be stored in a target data application of a controller belonging to the public sector - In contacts between natural persons and public bodies, the latter are allowed to store an ssPIN of the natural person and the natural person is allowed to store the sourcePIN of the public body
Belgium	- Yes
Bulgaria	- Yes
Cyprus	- The identity card number may be used.
Czech republic	- Yes, in accordance with "The Convention for Protection of Individuals with ..." – see ratification 09.07.2001)
Denmark	- Official authorities may process data concerning civil registration numbers with a view to unambiguous identification or as file numbers.
France	- Yes, for the social security organisations
Germany	- Tax identification number is only used for communication between the taxpayer and financial authorities in the tax procedure
Hungary	- Natural persons have no single identification numbers. - The single identification numbers of legal persons can be used by anybody without any restriction.
Ireland	- No answer
Italy	- No answer
Lithuania	- Yes
Luxembourg	- Yes
Malta	- Yes, as long as it is in line with article 18 of the DPA
Netherlands	- For the processing of personal data a national identification number can only be used for the implementation of the law which states that such a number may be used or for the purpose specified by law.
Spain	- Yes
Sweden	- Yes, with consent or based on any of the other grounds in section 9 of the PDA
United Kingdom	- No answer

Question IV.17

Assessment of the current legal situation concerning the sharing of identity data

Country	Documents
Austria	<ul style="list-style-type: none"> - Sharing of identity data will not be necessary in the future, since usage of the citizen card will provide authorised and standardised identification data legally approved by the sourcePIN authority by means of the identity link - The confirmed identification data could be incorporated into existing data applications as far as there is a legal foundation from the data protection point of view - According to the established system of the segmented public and private sectors, no controller has the power to merge data that should not be merged - The ssPIN can be used to track data records over an extended period of time without using any identifying information, which can make statistics more privacy-friendly
Belgium	<p>Drivers:</p> <ul style="list-style-type: none"> - Political statement that each administration, at federal level, should not ask identification data to citizens or companies of those data are already available in other federal administrations - Build up of the organisational and legal framework that enable the exchange of identity data between administrations - Build up of identity data exchange services on the Belgian middleware platform - Build up of authentication services for A, B, C <p>Projects:</p> <ul style="list-style-type: none"> - Build up of identity data store at European level
Bulgaria	<ul style="list-style-type: none"> - No answer
Cyprus	<p>Assessment:</p> <ul style="list-style-type: none"> - When there is a real need for the sharing of identity data, the matter is usually resolved by the grant by the Commissioner, of a combination license of the relevant filing systems. <p>Drivers:</p> <ul style="list-style-type: none"> - Having the correct information for identification purposes which in turn reduces the danger of mistaken identity either in the public or the private sector, is the main driver to the increase of sharing of identity data. Sharing of identity data is also important for the detection of crimes and Law enforcement purposes in general. <p>Projects:</p> <p>No</p>
Czech republic	<ul style="list-style-type: none"> - No answer
Denmark	<ul style="list-style-type: none"> - The Directive 95/46/EC has been incorporated into the Danish legislation - High attention is paid that the directive is incorporated into all public digitalisation projects. This of course limits the exchange of personal data but we assess that the considerations regarding the individual's legal rights and the right to protection of personal data that are laid down in the Directive 95/46/EC are more important. - We do think that it is important continuously to assess the individual's legal rights compared to the individual's experience of the public service as effective and having a high quality.
France	<ul style="list-style-type: none"> - The law on the private data protection may be considered as an hindrance but this is necessary
Germany	<p>Assessment:</p> <ul style="list-style-type: none"> - The reasons for existing hindrances are justified. Generally, there is no need for change. - The sharing of identity data is only needed in some special cases. - Modern technical authentication depends on cryptographic keys that have a duration of approx. five years only.
Hungary	<p>Assessment:</p> <ul style="list-style-type: none"> - Legal persons: no hindrances. - Natural persons: the privacy law makes sharing of identity data very difficult. <p>Drivers:</p> <ul style="list-style-type: none"> - New law for public administration processes enforcing the online case management, driving force for sharing identity data electronically <p>Project:</p> <ul style="list-style-type: none"> - Executive decrees of the new law for public administration processes is under preparation,
Ireland	<p>Driver:</p> <ul style="list-style-type: none"> - e-Government initiative
Italy	<ul style="list-style-type: none"> - No answer

Lithuania	<p>Assessment: The system of unique personal identification should be amended either by providing for a system of sector based identification or limiting the justified processing of the PIN by the law. Additionally the number of legal persons indicated in Art. 7 (3) 4 of the Law on LPPD should be reduced to the necessary cases.</p> <p>Drivers: The need for information, the need to identify accurately the person's identity providing certain services.</p> <p>Project: At the present the SPDI prepares the draft of the Art. 7 of the Law on LPPD limiting the scope of the subjects who have the right to use the personal identification number.</p>
Luxembourg	- Pending reflections
Malta	<p>- As long as the sharing of identity data is done in a legal and lawful manner as explained in the above questions, no legal hindrance is made.</p> <p>- When such identity data is however tied to sensitive data, and it is specifically prescribed by law that such information cannot be divulged, such sharing of information has to be withheld.</p>
Netherlands	<p>Projects:</p> <ul style="list-style-type: none"> - Sharing of data is handled in a collection of projects that intend to realize 'basic registers' concerning six different registers (in the future another five will be added). - Ongoing work on the implementation of a Civil Servant Number
Spain	<ul style="list-style-type: none"> - The personal data protection is well developed, including the security measures needed for each type of personal data - The protection of personal data is relevant to the Criteria for Security, Normalization and Conservation, which are compulsory for the full legal value of electronic and telematic administrative procedures
Sweden	<p>Assessment: - The regulation lacks an overarching information resource perspective. This has resulted in fragmented legislation, and different technical and administrative solutions in different sectors.</p> <p>Drivers: - Financial drivers and the strife for efficiency and better services.</p> <p>Projects - Ongoing discussions regarding increased possibilities for exchange of data between authorities that handle allowances, such as social insurances, social welfare etc., in order to avoid fraud situations. - A proposal for a new Secrecy Act also contains rules that would open up for increased possibilities to exchange data for example about young people between social welfare authorities and the police for the purpose of preventing them from committing crimes.</p>
United Kingdom	<p>Assessment: - Complex: The regime does not, in most circumstances, prevent the sharing of data, but is often perceived as if it does.</p> <p>Drivers: - Joined-up government and the provision of personalised public services - Organised crime and national security areas</p> <p>Projects: - See Guidance on Public Sector Data Sharing</p>