A Model for Electronic Data Exchange in the Public Sector

Frank Robben

A fluid electronic data exchange between public services is an important condition for an efficient and effective functioning of these services and for preventing citizens and companies from superfluous administrative formalities. This paper presents a model and some basic information security measures in order to organise electronic data exchange between public services in accordance with the finality principle and the proportionality principle stated within the regulation on data protection.

I. The problem

1. Most countries have an elaborate system of public services for which information is a very significant input. This information is needed to collect taxes, award benefits or subsidies, manage population and company registers, and so on. Moreover, the various public services often need the same information: identity data, data on familial or social situations, data on wages and working hours, etc. Likewise, the result of the processing of information by a public service is regularly of importance to another public service. Thus, social security status can, for example, be relevant for the enjoyment of certain tax rebates.

Likewise, it is necessary that the public services ensure a fluid mutual exchange of electronic data. In the absence thereof they work inefficiently and probably ineffectively, and burden citizens and companies with superfluous administrative formalities. Citizens and companies then have to provide the same information several times over to different public services, often each time according to other instructions, or have themselves to send information which they have obtained from one public service, to another public service.

2. The mutual exchange of data between public services must be organised in such a way that each public service can gain easy access to information which they need and which another public service already has. But to the same extent, it must be guaranteed that a public service cannot gain access to information which is not relevant for the execution of its own task.

Respect for this so-called proportionality principle is imposed in any case, by the European Directive on the protection of individuals with regard to the processing of personal data, which states that personal data can only be processed to the extent that it is adequate, relevant and not excessive in relation to the purposes for which such data are collected or processed. The same directive also demands that data be obtained for specified, explicit and legitimate purposes and not be further processed in a way that is incompatible with those purposes (the so-called finality principle).

Striving towards a single collection of information from citizens and companies must not lead to these principles becoming devoid of all meaning. The government must offer structural guarantees for the respect of these principles with the mutual exchange of electronic data between public services. At the same time these principles cannot be defined so strictly, that an efficient data exchange between public services is restricted unnecessarily. Here the organs which are responsible for the interpretation and implementation of the rules on the protection

of privacy, both on the national and supranational level, have a significant responsibility. This is still not always realised. All too often, the meaningful re-use of data by public services is still rejected on the grounds of a perceived incompatibility.

In the examination which follows, a method for, and organisation of, the security of information is presented, by which electronic data exchange between public services can be organised with respect for the aforementioned principles. The model, and the organisation, of information security has been successfully implemented in the Belgian social security system.

II. The proposed model

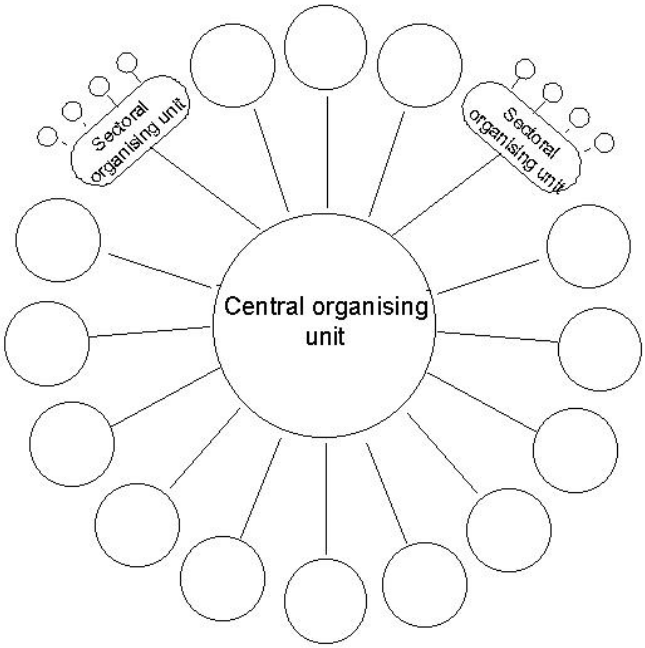
A. A network managed by a central organising unit

3. The model is based on a network that is managed by a central organising unit, from which the mutual data exchange is organised and regulated, and to which all public services are directly or indirectly connected. Different network typologies are possible, but the most appropriate one is the star-shaped network structure.

Preferably, the central organising unit will be an institution founded especially for that purpose, which is sufficiently independent from the other public services and has no other substantive tasks. When tasks other than the organisation and regulation of the data traffic are awarded to it, the central organising unit will itself need to have the data at its disposal in order to execute these tasks, thus creating a situation in which the unit would be judge and jury. This would not benefit its authority and independence. The public services would regard it as biased and they would lack the confidence necessary for the network to be efficient.

If such a large number of public services are involved in one country, to the extent that it makes centralised management of the mutual data traffic by the central organising unit almost impossible, sectional organising units can be set up to organise and regulate the data traffic within a sector of the public service providers (social security, tax, ...). In this case, the central organising unit will only provide for the organisation of the data traffic between the different sectors of the public services.

4. The network structure can be illustrated schematically as follows.



B. The unique identification key

5. If public services exchange data relating to persons through the network, they have to be sure they are referring to the right and the same person. Consequently it will be preferable to have each person identified by the different public services using the same unique identification key. This identification key preferably remains unchanged through time, and thus may not be changed when certain characteristics of the identified person change. Every adaptation of the identification key requires a synchronised updating of the databases of all public services which have a file on the person involved. In order to enhance the stability of the identification key and to respect the privacy of the person involved, the key should consist of a sequential number with no substance.

6. Moreover, each person should have an official document mentioning the identification key in the most reliable way, preferably readable visually and electronically.
Firstly, in this way, the person will have an easier access to the public services. It is sufficient that he presents his unique identification key to whatever public service in order to (electronically) consult his file. The dragging around of file numbers belongs to the past. Moreover it is easier for the public services to ask each other for information on the citizen. Without a unique identification key the citizen would have to be identified by identification data containing information such as the name, date of birth or address, with a much greater risk of mistakes being made. Thanks to the easier data exchange between public services the citizen and the companies are relieved from a lot of paperwork when transmitting information to the public services. They do not have to transmit the same information to the large number of different public services over and over again.

C. The reference directory

7. For an optimal management of the network, the central organising unit (and each sectoral organising unit) should use a relational database containing no information on the content.

This database would only include reference data per person indicating what data is kept in which sector(s) or public service(s) and what data can be obtained.

In other words such a reference directory should be made of at least three different interrelated charts:

(a) a directory of persons (who-where-how-when-chart) mentioning for each person to whom a file is related, their capacity as well as the public services where a file is kept and for what periods;

(b) an availability chart (what-where chart) with the data available in the different types of public services with regard to the different types of files;

(c) an access authorisation chart (who gets what chart) mentioning the data that the different public services can obtain with regard to the different types of files.

8. The directory of persons and the availability chart of the reference directory are provided with information by the different public services. Each public service thus provides the information pertaining to for which persons they have what kind of files and for what period of time, and what kind of data is available in the different kinds of files. The data itself is of course not included in the charts.

The access authorisation chart is made up by an independent organ, appointed by Parliament, which supervises the respect for the basic principles of the protection of privacy, in particular the finality principle and the principle of proportionality, via electronic exchange of data.

9. The reference directory has three functions. First of all this directory constitutes the basis for a preventive control on the regularity of the access to information in the network, and thus on the respect of the finality principle and the principle of proportionality whenever data is exchanged. The access authorisation chart can be used to verify whether an institution which desires information may receive it; the directory of persons can be used to determine if a person, about whom an institution wishes to receive information, actually has a file in that institution.

Secondly, the reference directory is used to route information to the right institution. The availability chart can be consulted in order to determine where the desired information is stored and the directory of persons can be consulted to verify whether the person about whom information is asked really has a file at that place.

Thirdly the reference directory also allows the central organising unit to transmit automatically certain information at its disposal, such as a change of address, to the requesting institutions. The directory of persons can be used to determine which institutions keep a file on the person involved.

D. Data collection

10. If a public service needs but does not yet have certain information concerning a particular person, it will first have to apply through the network to the central organising unit, via the sectoral organising unit, as the case may be. The same procedure will have to be followed when an institution wants to check the correctness of the data. Needless to say, this procedure will not have to be followed if the institution concerned has the task of keeping the

information up to date according to the functional competence distribution concerning data storage, which will be described later.

When information is requested, the central organising unit first checks the validity of the request using the access authorisations chart and the persons directory of the reference directory.

If the requested information may be transmitted, the central organising unit will consult the availability chart and the persons directory of the reference directory in order to determine if the data is already available in the network, and, that being the case, where it can be obtained. If the information is present in the network, the central organising unit automatically collects it in the supplying institution (electronically), and transmits the data to the interested party. When the data are not available in the network the interested institution will be authorised to question the citizen or other persons who can supply the information in question (for instance, the employer). In order to update the reference directory the institution in charge of collecting data communicates the result of the interview to the central organising unit, via the sectoral organising unit, as the case may be. The central organising unit transmits this result automatically to the institution responsible for data storage.

The goal of the method described above is to have a single collection of basic data from citizens and companies in order to relieve them, to a great extent, of many administrative formalities.

E. Data storage

11. Normally, the central organising unit does not contain any data related to the content. It only refers to information stored in a decentralised and distributed way.

After having consulted the different public services or sectors, the central organising unit can distribute functional competencies concerning data storage between public services.

The institution in charge of storing a category of data must store this information and, if necessary, keep it up to date according to the needs of all the public services. This public service thus operates as the authentic source of this category of data. The other public services that require these data only have to keep this information until the end of their tasks. They will not have to ensure that the history of it is noted.

Moreover when distributing data storage responsibilities the distribution of competence with respect to content between the different public services has to be taken into account as much as possible.

F. Data exchange

12. Normally, each exchange of personal data coming from a public service must pass through the central organising unit. To avoid endangering the efficient functioning of the public services to too great an extent, several exceptions to this rule could be foreseen. For instance one could suppress the obligation of passing through the central organising unit for the communication of data to the citizen or their employers themselves or for the exchange of data between institutions of the same sector organised through the sectoral central organising unit.

13. The initiative to exchange data through the network can be taken by the institution that needs information, by requesting the information, but also by the institution in the possession of this information, by transmitting certain data. In this context, it is preferable with regard to certain data, to have certain data modifications automatically communicated to the interested institutions. For instance, when a citizen has a new address, the central organising unit, which will be informed of this by a public service and after having consulted the reference directory, could transmit the new address to all public services that keep a file related to that citizen or which are interested in this data modification.

III. Data protection

14. As mentioned above, the rationalisation of the administration through the encouraging of the re-use of data has to be accompanied by the necessary measures as to data protection. Such protection relates to at least three aspects:

- guarantee of data availability: to prevent data from being inaccessible or wrongfully erased;
- guarantee of data integrity: to prevent data from being wrongfully modified;
- guarantee of data confidentiality: to prevent data from being processed by unauthorised users or for unauthorised purposes.

The elaboration of a consistent and coherent security system has to be based on a number of general points of departure, which will then be converted into a logical set of structural, institutional, legal, organisational and technical measures, which relate to the three aforementioned aspects. It is not within the scope of this article to examine in depth the general principles and the set of measures. Nevertheless, in light of the above presentation of the problem, the measures which can improve the guaranteeing of one aspect of data protection, i.e. the guaranteeing of the confidentiality of the data, are briefly discussed.

A. The structural protective effects resulting from the model

15. The presented model first of all offers a number of structural guarantees concerning the protection of the confidentiality of the data. A centralised data storage is avoided to the extent possible. The data are kept in the different public services and thus in several places. The central organising unit only keeps the references to the places where the data is kept, without saving the data itself. An unauthorised access to the central organising unit itself can thus in no case cause a significant number of data concerning a person to become available. The option for a distributed data storage, according to a functional distribution of competence between the public services, limits the degree of availability of information and thus reduces the risk of misuse.

Furthermore in the network concept, public services can only communicate personal data to each other or to a third party if the validity of the data transfer has been controlled by the central organising unit. This unit also necessarily has at its disposal, the required logging data in order to detect (attempts at) misuses or attempts to intrude the network.

B. Institutional measures

16. The protection of an information system is not in the first place a technical product, which can be built into the system by experts, but rather it is a result of the careful execution of the daily task of every person involved in the functioning of the system. An efficient security organisation is therefore of primary importance. Such an organisation should be institutionalised.

17. A first useful measure related to it is the foundation, in each public service, of an internal information security service in charge of advising, stimulating, documenting and controlling as far as information security is concerned. In this way, permanent attention will be guaranteed in every service regarding information security. More precisely, this organ advises the person responsible for the daily management, on his request or on its own initiative, of all the aspects of information security. The advice is motivated and communicated in a written form, save in the case of very limited risks. If the person responsible for the daily management departs from the written advice, he must inform the information security service through a letter, motivating this. Thanks to this procedure, the information security service will receive the necessary feedback regarding the adopted measures and the daily management becomes more responsible as far as information security is concerned.

Moreover, the information security service draws up a security plan spread over several years for the person in charge of the daily management, mentioning all the tools required for its execution. This plan is updated each year.

Finally the information security service offers a yearly security report to the daily management that gives a general survey of the security situation, the evolution in the past year, the objectives that still have to be realised and also the results of the controls made by the information security service, including a description of all the events that might have endangered the information security of the institution or the network, and the proposed measures.

18. For a good co-ordination between information security consultants in the different public services, a co-ordination group "Information Security" can be set up presided over by the information security consultant of the central organising unit. Moreover, within this co-ordination group, documentation necessary for a better fulfilment of the tasks of the internal information security services can be gathered. It can also propose minimal norms related to the physical and logical information security which must be observed by every public service.

19. The internal information security services must be versatile with regard to information security. Nevertheless they will sometimes need specialist advice or help with regard to certain aspects of information security. In order to meet this need, it might be useful to set up or authorise one or more specialised information security services for the whole public sector, with specialists working in various information security sectors, that could be consulted by internal information security consultants when they need more specialised support. In addition to this specialised support, the specialised security service could also organise training, support and follow-up awareness campaigns or even undertake research and audits, at the request of a public service.

20. Besides the internal information security service and the possible specialised information security services, it might be desirable to organise an independent external supervisory organ. This external supervisory organ should be designated by the Parliament and the members

thereof should satisfy strict criteria in order to be fully independent, with regard to public services, directors, and supervisory boards. This independent control organ can be the same as that which was recommended in point 8 with regard to the completion of the access authorisation chart of the reference directory. Furthermore, the external supervisory body can also be engaged to make sure that public services observe security measures. In order to fulfil this task correctly, the external supervisory body must have a broad authority to investigate. Moreover, in such investigations, the external supervisory body must be able intervene on its own enterprise or in response to a complaint. Any person, in particular any employee of a public service, must be able to apply to this supervisory body, without the need for any prior authorisation in order to communicate facts or situations that would justify the intervention of the supervisory body. Apart from the person concerned giving a formal permission, the name of the complainant may not be disclosed. The external supervisory body must also be able to formulate recommendations or advice, on its own initiative or on request, with regard to the execution of security measures. The external supervisory body must be able to take cases to court, when it finds that public services have not respected security measures demanded in law. Finally the external supervisory body should draw up a detailed activity report for Parliament every year, that can be consulted or obtained by any interested party.

C. Organisational and technical measures

21. The institution of the bodies described above, must ultimately ensure that a coherent system of effective organisational and technical security measures is applied. This system of measures should be based on an analysis of possible threats. A number of effective organisational and technical measures should be set up to prevent or alleviate each possible threat. Efficient procedures of mutual information exchange between public services must be defined, by which services who fall victim to such a risk can inform other services – that may be susceptible to consequential risks - in good time .

D. Physical threats

22. These threats have a natural or chemical origin, such as fire, smoke, water, humidity, variations in temperature, … Such phenomena can seriously damage information systems. The institutions must therefore take the necessary measures in order to avoid such risks (for instance, by having no sources of ignition or inflammable materials in the computer rooms), good detection systems, and efficient means and methods – which are tested and practised regularly - to fight against such risks should they be realised.

E. Logical threats

23. Logical threats do not have a natural or chemical origin. These threats arise from the information system itself, or its own users.

1. Unauthorised access and processing

24. An efficient control system must be set up to supervise the access to every component of the information system: the different hardware components, the system software, the application programmes, the data, … Access profiles must be defined for each of these components. These profiles correspond to three questions:

- who is allowed to use the component ?
- from which environment, and during which periods of time can the user use the component ?

- which operations can be executed by the user (additions, modifications, omissions, executions, …) ?

The access control must be based at least on an identity check (who are you?) and authenticity check (to prove that you are who you claim to be). Authenticity can be proved by means of knowledge (e.g. a password), possession (e.g. a chip card), biometric characteristics (e.g. the voice or fingerprints) or a combination of these.

Detection mechanisms must be incorporated in order to detect and report any unauthorised access (or attempted unauthorised access).

Data that could be subjected to unauthorised manipulations should be encrypted.

2. Deterioration of quality and integrity

The necessary guarantees must be taken for a good functioning of the various components of an information system and to prevent their unauthorised modification.

First of all, information systems must be protected against (unintentional) errors. This protection can, for example, be achieved by the implementation of an efficient quality control system, through which the necessary procedures are determined in order to check every stage of data processing, from its inception, to the programming, and to the actual exploitation of the data. A good documentation can help to correct errors quickly.

An information system can be the subject of many forms of intentional damaging human conduct: theft of hardware, data, or programmes, sabotage or intrusion into information systems, the transmission of computer viruses, ... In this case preventive measures (such as the aforementioned access control, the division of functions, the compartmentalisation, …), detection measures (such as the taking and use of loggings, the maintainance of permanent inventories of hardware components, …) and recovery measures (such as properly documented and regularly tested recovery facilities) are also necessary.

Within the context of intentional damage, one must be particularly attentive to the staff in every public service, for they have the most opportunities to act – be it not intentionally – in a damaging way. The staff must be sensitised, motivated and trained with regard to the security issue. Appropriate security measures must be adapted whenever a staff member leaves, resigns, is transferred or absent. Finally, one must avoid incoherence concerning the tasks of a person, for instance, a person cannot execute and control at the same time.

Main references

- Kruispuntbank van de Sociale Zekerheid, *Kruispuntbank van de Sociale Zekerheid. Het telematicanetwerk van de sociale zekerheid 1998-1999*, Brussel, Kruispuntbank van de Sociale Zekerheid, 2000, 252 p.

- http://www.ksz.fgov.be