INTERNATIONAL SOCIAL SECURITY ASSOCIATION
ASSOCIATION INTERNATIONALE DE LA SÉCURITÉ SOCIALE
ASOCIACIÓN INTERNACIONAL DE LA SEGURIDAD SOCIAL
INTERNATIONALE VEREINIGUNG FÜR SOZIALE SICHERHEIT

International Conference on Information and Communication Technology in Social Security

ICT as a cornerstone of integrated and citizen-centred social security

Brasilia, Brazil, 17-20 April 2012

Privacy and protection of personal data in the use of information and communication technologies in social security systems

Rodrigo Moya García
Head of Planning and Development Unit
Superintendents' Office of Social Security
Chile

ISSA/ICT/CONF/BRASILIA/12

Privacy and protection of personal data in the use of information and communication technologies in social security systems[1]

Rodrigo Moya García
Head of Planning and Development Unit
Superintendents' Office of Social Security
Chile

1. Issues arising in the processing of personal data in Social Security systems

The necessary starting point for this paper is to avow the importance that the use of databases by public institutions has acquired in the modernization of the State in general, and in the development of information systems to improve the processing and control of social security regimes in particular. Over the years, we have seen how government makes increasing use of databases, above all as ICT tools for the efficient administration of archives and the retrieval of data contained in documents.

However, the servers of the different public bodies are not only replete with documentary databases, but also, and even more importantly, with personal records or data banks, which are personal in the sense that they contain information referring to identified or identifiable individuals.

Many of the key issues concern this type of personal data and especially the use that different public social security agencies make of them, bearing in mind that all processing of these databases and the data they contain must necessarily comply with the current law. The problem is that on occasions legislators have not clearly defined the scope of the regulations with respect to government, that is, when the agency processing the data is a public body. Hence the numerous lacunae currently found in the legislation and the risk scenarios these create.

[1] Paper to be delivered at the International Conference on Information and Communication Technology in Social Security, organized by the International Social Security Association (ISSA).

* Rodrigo Moya García is a Chilean lawyer. He holds a degree in Law and Social Sciences, a diploma in Computer Studies, and a Masters in Public Law from the Law Faculty at the Universidad de Chile. An Assistant Professor in the Department of Computer Law at his alma mater, he has researched and written numerous studies and publications on the relationship between the law and ICT. He is currently serving as Head of Planning and Development in the Superintendents' Office of Social Security, specializing in the regulation of information systems. He has been responsible for a number of projects directly related to the processing of personal data and privacy in social security ICT systems.

2. The Development of databases in public agencies in the field of Social Security

One of the main issues is to establish on what legal grounds a public agency working in the field of social security may keep databases of personal records. In this respect it is first necessary to state very clearly that, in the Chilean case, if a public body creates a database merely as a tool for internal data processing, that is, not as an end in itself, but merely as a means to an end, it does not require any kind of special authorization to do so. The instrumental character of the database means that the establishment of databases in general, and databases with personal information in particular, is the sovereign decision of the public agency in question. Public bodies are only required to comply with their legal obligations, to ensure that any data processing is carried out in accordance with the law and within the scope of their authority, and to fulfil the obligations derived from possession of the database.

In contrast, it should be stressed that legal authorization is required to compile records that could give rise to rights and duties for individuals, insofar as the information pertains to the individual. In other words, a personal information database may be used to generate a public record, and legal authority is required to create this record (even if not to create the database itself).

Nonetheless, it is also necessary to consider the legal basis and mechanisms used for data capture. The procedure used to collate personal data must be duly informed, transparent, and legally justified. Compliance with these norms will help determine the legality and legitimacy of the resulting database and whether any future processing of the personal data will be carried out in accordance with the principles of legality and due purpose.

Once a public social security agency has created a database of personal information, that body becomes responsible for the records and databank, insofar as it has decision-making power with respect to processing the personal information contained therein. Hence the agency's obligation to protect the data with due diligence and assume responsibility for any harm resulting from them. Equally, when the data in question have been obtained from sources not accessible to the general public, the personnel who work in data processing in public bodies are obliged to keep the data secret, as well as to respect the confidentiality of all other data and information related to the data bank. It should be noted that this obligation to secrecy and confidentiality continues to hold even after a civil servant stops working with the data in question.

3. Regulation of personal data processing by public bodies

In Chile, the processing of personal data is presently regulated by Law 19,628, and more particularly by its Section IV "On data processing by public bodies". This comprises three articles which lay down a number of rules specifically referring to the processing of personal data by government bodies. Article 20 of the law is especially significant. This establishes that "A public agency may only process personal data relevant to its sphere of responsibility and in compliance with the rules set out above. In these conditions, individual consent is not required".

This is the core precept and mainstay of all discussion regarding the processing of personal data by public agencies.

A public body may, without restriction of any kind, process anonymous data, that is, as long at the data (whether due to the nature of the source or the way it is processed) cannot be

linked to an identified or identifiable individual. Anonymous databases are of enormous importance due to their use in compiling statistics, and in analysis and research, and as such they may be communicated to third (private or public) parties and published without restriction.

Thus, in the case of personal data, in accordance with Article 20 of Law 19,628, a public body is permitted to process these within its sphere of competence as it sees fit. It does not require any type of specific authorization to process personal data, as long as this operation falls within its legally defined sphere of responsibility and competence. That said, the agency´s competence must be direct and related to the data in question.

In the same way, and as has been confirmed by the Comptroller's Office of the Republic of Chile, the fact that a public agency is allowed to process personal data (through any operation or series of operations or technical procedures, whether automated or otherwise) in pursuit of its legitimate objectives, does not mean that it is entitled to pass this information on to third parties. The legality or otherwise of data exchange depends on the nature of the data and responsibilities of the agency in question.

Generally speaking, therefore, a public agency may process personal data (and, as a result, communicate this to third parties), without the individual's consent as long as it respects the following principles:

- The principle of legality: the data transfer must fall within its sphere of responsibility.
- The principle of purpose: the agency must ensure that any data transferred to third parties are only used for purposes coherent with that for which they were collated.
- Principle of responsibility: the public agency must fulfil its obligations as the body responsible for the personal records or data bank.

4. Personal data privacy and ICT security protocols

As noted above, the different public agencies operating in the field of social security develop databases as tools for their internal operations, whether:

- to improve the management and monitoring of claims or requests for information made by users or legal entities;
- to facilitate the processing and settlement of cases;
- to contribute to the effective regulation and scrutiny of the different employment and social security regimes for which they are responsible;
- to optimize the payment and control of welfare benefits; and
- to produce reports and statistics on subjects that fall within their areas of responsibility.

In the light of all this, there is a need to devise a policy on data security in social security systems. This should serve to ensure compliance with the obligations arising from the necessary personal data security and privacy standards and, at the same time, guarantee the availability of the data to those institutions and entities which need them in order to fulfil their duties.

On this point it is important to clarify that in Chile, specific legislation does exist with respect to the security of electronic documents. This is Decree 83, which sets out the technical rules on the security and confidentiality of electronic documents in government bodies. The obligations and recommendations laid out in Decree 83 are intended:

- to guarantee minimum standards of security in the use, storage, access and distribution of electronic documents;
- to facilitate the use of electronic communication between public agencies and bodies and between these and citizens and the private sector in general; and
- to ensure that electronic documents can be used safely, trustworthily, and in full compliance with the existing legislation on the confidentiality of the data exchanged.

On the other hand, since 2010 "Information Security" systems have come within the remit of the Department of "Quality of User Services", the support and approval of which is the responsibility of the Undersecretariat of the Ministry of the Interior and the Department of Budgets. As explained in the Ministry´s internal manual, "data constitute an asset which, like the organization's other assets, is of great value and must be safeguarded accordingly. Information Security protects this data from threats of many different kinds in order to ensure the continuity of the operations, minimize the risk of any damage arising to the institution, and maximize the efficiency and the opportunities for greater efficiency".

In this context, it is suggested that the Information Security is achieved by implementing an appropriate series of controls, in the form of policies, procedures, practices, organizational structures and software. All public agencies need Information Security Systems capable of guaranteeing the quality, availability, and adequacy of the data they hold.

The basic premise for such systems is that the safety of electronic documents is achieved by guaranteeing a series of essential attributes, namely confidentiality, integrity, authentication, and reliability.

For confidentiality to be assured the contents of electronic documents must only be accessible to authorized persons, implying the need to establish clearly whether documents are public, reserved, or secret. The integrity of electronic documents means that public agencies must introduce measures to ensure the completeness and accuracy of such documents and the data processing methods used, as well as of any changes made to the documents by duly authorized authorities. The need for a viable means of authentication implies that all authors of electronic documents and users of a database must be required to identify themselves. Reliability, finally, signifies that authorized users must have adequate access to the electronic documents and the means to process them.

5. Proposed solution

All this points to the need to analyse the appropriate security policies with respect to data collation, storage and processing by public social security authorities. Any consideration of this question must take account of the fact that these data are, quite logically, not just for internal use, but also required for studies, research, control and the generation of public policies. The data exchange that for these purposes inevitably takes places between different bodies constitutes an important object of analysis. In this sense, it is instructive to consider the main issues at stake in the ongoing debate in Chile (issues which are compelling, closely related and of great public interest):

- Data transfer and exchange between public bodies.
- Efficient operation of the State´s integrated platform of electronic services.
- Conflicts between the obligation to protect personal data, on the one hand, and to guarantee access, to and the transparency of, public information on the other.
- Operational issues deriving from a public body's obligations to guarantee the quality and security of data.
- Processing of personal data obtained though surveys carried out by public bodies.

As it would be much too lengthy to analyse each of these issues here (they will be considered in depth in the conference), the model of good practices in data security proposed in this paper focuses on four key instances in which public agencies in the field of social security require rigorous protocols in order to ensure the implementation of an effective security policy. Let us consider each of these in turn.

Protection in the processing of personal data

"Protection in processing" implies that all public bodies and agencies which handle individuals' personal data need to introduce safeguards to ensure that these are processed in strict accordance with the law.

More specifically, with respect to:

- Capture: public bodies should only capture data relevant to their duties and responsibilities or obtained by other agencies with responsibilities in the same field. Data should not be used for purposes other than those for which they were originally obtained.
- Storage: data must be stored securely (with both physical and logical safeguards) to ensure that it cannot be accessed by unauthorized third parties.
- Processing: data processing must strictly adhere to the existing regulations on the privacy and protection of personal data. Accordingly, only disassociated or anonymous data should be published or communicated, and nominal information should only be transferred between public bodies with responsibilities in the field and under strict security protocols (within the framework of a cooperation agreement between the two bodies).

Protection of documents

The requirement to guarantee the protection of documents themselves would appear to advise the use of the official standard of electronic documents, in XML format, in the terms set out in the Ministry of the President's Office's DS 81 (2004) on the interoperability of electronic documents.

These standards would appear to resolve the problems arising with respect to various key requirements for electronic documents in XML format, namely those of authenticity, integrity, non-repudiation and, most importantly, confidentiality. This can be achieved through the use of the use of PKI, XML, Signature, XML Encryption or biometric mechanisms.

On the other hand, at the level of ICT systems, the best technological model is that offered by service-orientated architecture, integrating as it does Web Services which permit the retrieval of electronic documents in XML and the use of native XML databases to store these documents. XML electronic documents, in turn, should be generated in accordance with an XML Schema, the structure and content of which should be defined by each relevant body depending on its individual needs and responsibilities. These innovations would also help guarantee the quality of the data received.

Institutional Protection

Institutional protection highlights the need for public bodies to adopt full control and security mechanisms to protect their technological hardware infrastructure and software. They must comply with the standards and requirements set out in DS 83.

These requirements are well-documented, and this is not the place to consider them in detail. All that is needed is for further progress to be made on the systematization of the standards and control of compliance.

Contractual Protection

In this context, it should also be noted that many public bodies have externalized their data storage centres, contracting out to external providers the hosting, support and maintenance of their various ICT systems. In this context, an effective data security policy also requires establishing obligations in this respect for technology suppliers. These should be clearly set out in the invitation to tender and the terms under which such services are contracted.[2]

[2] **General Security**: storage of passwords; response of the ICT system to breakdowns; validation of data entry in the information system; non-indexation by search engines; communication through secure channels; completeness of programmes and data; automatic disconnection; register of logs; and monitoring system. **Access**: Time synchronization; security of access to infrastructure. **Storage**: capacity, redundancy. **Back-up**: in the data centre, back up outside the data centre, security of access to the back-up; state of the back-up infrastructure; reset procedure; time of recovery of the information and data. **Levels of service**: Up Time, contingency management; support and maintenance. On the other hand, it is especially important to include specific clauses, both in the invitation to tender and in the contracts made with suppliers of technological services. These should cover the following issues: **the obligation to secrecy, safeguard and protection**: clauses on confidentiality and protection of personal data and intellectual property. **Sanctions for non-compliance**: clauses governing the withdrawal of contract, guarantee of full compliance with the contact and fines for non-compliance.